

Red Hat Network Satellite 5.5 Benutzerhandbuch

Verwendung und Verwaltung des Red Hat Network Satellite
Ausgabe 2

Landmann

Red Hat Network Satellite 5.5 Benutzerhandbuch

Verwendung und Verwaltung des Red Hat Network Satellite
Ausgabe 2

Landmann
rlandmann@redhat.com

Rechtlicher Hinweis

Zusammenfassung

Dieses Buch beschreibt die Verwendung und den Betrieb des Red Hat Network Satellite. Weitere Informationen finden Sie im Red Hat Network Satellite Handbuch zum Einstieg.

Inhaltsverzeichnis

Vorwort **4**

Kapitel 1. Benutzerverwaltung **5**
1.1. Hinzufügen, Deaktivieren und Löschen von Benutzerkonten 5
1.2. Benutzerverwaltung 9

Kapitel 2. Automatische Synchronisation **11**

Kapitel 3. Datensicherung und Wiederherstellung **12**
3.1. Datensicherung 12
3.2. Wiederherstellung von der Sicherungskopie 13
3.3. Automatisierte Datensicherung 14

Kapitel 4. Klonen einer Maschine **16**
4.1. Funktionsumfang 16
4.2. Befehlszeilenoptionen 16
4.3. Beispielverwendung 18

Kapitel 5. Monitoring **19**

Kapitel 6. OpenSCAP **20**
6.1. OpenSCAP-Funktionsumfang 20
6.2. OpenSCAP in RHN Satellite 21
6.2.1. Voraussetzungen 21
6.2.2. Durchführen von Prüfscans 21
6.2.3. Anzeigen von SCAP-Ergebnissen 24
6.2.4. OpenSCAP Satellite-Seiten 24
6.2.4.1. Prüfen 24
6.2.4.2. Systeme → Systemdetails → Prüfen 27

Kapitel 7. PAM-Authentifizierung **31**

Kapitel 8. RPMs **33**

Kapitel 9. Boot-Geräte **36**

Kapitel 10. Organisationen **41**
10.1. Erstellen von Organisationen 42
10.2. Verwalten der Berechtigungen 43
10.3. Konfigurieren von Systemen in einer Organisation 44
10.4. Benutzer einer Organisation 45
10.5. Organisations-Trusts 46

Versionsgeschichte **50**

Stichwortverzeichnis **52**
A 52
B 52
D 52
E 52
F 53
H 53
K 53
L 53

O 53
P 53
S 53
V 54
W 54

Vorwort

Red Hat Network bietet Unterstützung und Verwaltung von Red Hat Systemen und Netzwerken von Systemen auf Systemebene. Es vereinigt die Werkzeuge, Dienste und Informationsquellen, die dazu nötig sind, die Zuverlässigkeit, Sicherheit und Leistung Ihrer Red Hat Systeme zu maximieren. Um das Red Hat Network einzusetzen, registrieren Systemadministratoren Software- und Hardware-Profile Ihrer Client-Systeme, auch System-Profile genannt, beim Red Hat Network. Wenn ein Client-System eine Paketaktualisierung anfordert, werden nur die auf diesen Client passenden Pakete ausgegeben.

Red Hat Network Server ermöglicht es Unternehmen, die Vorteile vom Red Hat Network zu nutzen, ohne öffentlichen Internetzugang zu ihren Servern oder Client-Systemen bereitstellen zu müssen. Systemprofile werden lokal auf dem Satellite-Server des Kunden gespeichert. Die Red Hat Network Satellite Website wird von einem lokalen Webserver bereitgestellt und kann nur von Systemen aufgerufen werden, die Zugriff auf den Satellite haben. Sämtliche Aufgaben zur Paketverwaltung, einschließlich Errata-Updates, werden über den Satellite-Server durchgeführt.

RHN Satellite Server stellt eine Lösung für Unternehmen dar, die vollständige Kontrolle und Datenschutz bei der Paketimplementierung und der Verwaltung ihrer Server verlangen. Er ermöglicht Red Hat Network Kunden die größtmögliche Flexibilität und Kontrolle bei der Sicherung und Aktualisierung von Systemen. Es können Module zum Satellite-Server hinzugefügt werden, um zusätzliche Funktionen zu ermöglichen. Dieses Dokument liefert einen Leitfaden für Operationen, die für den Betrieb des Satellite-Servers wesentlich sind.

Kapitel 1. Benutzerverwaltung

1.1. Hinzufügen, Deaktivieren und Löschen von Benutzerkonten

Benutzer können über den **`Benutzer`**-Reiter oben in der RHN Satellite Server Navigationsleiste verwaltet werden. Auf diesem Reiter können Benutzerrechte vergeben und bearbeitet werden.

Prozedur 1.1. Benutzer hinzufügen

Um neue Benutzer zur Organisation hinzuzufügen:

1. Klicken Sie oben rechts auf dem **`Benutzer`**-Reiter auf **`Neuen Benutzer anlegen`**, um die Seite **`Benutzer anlegen`** zu öffnen.

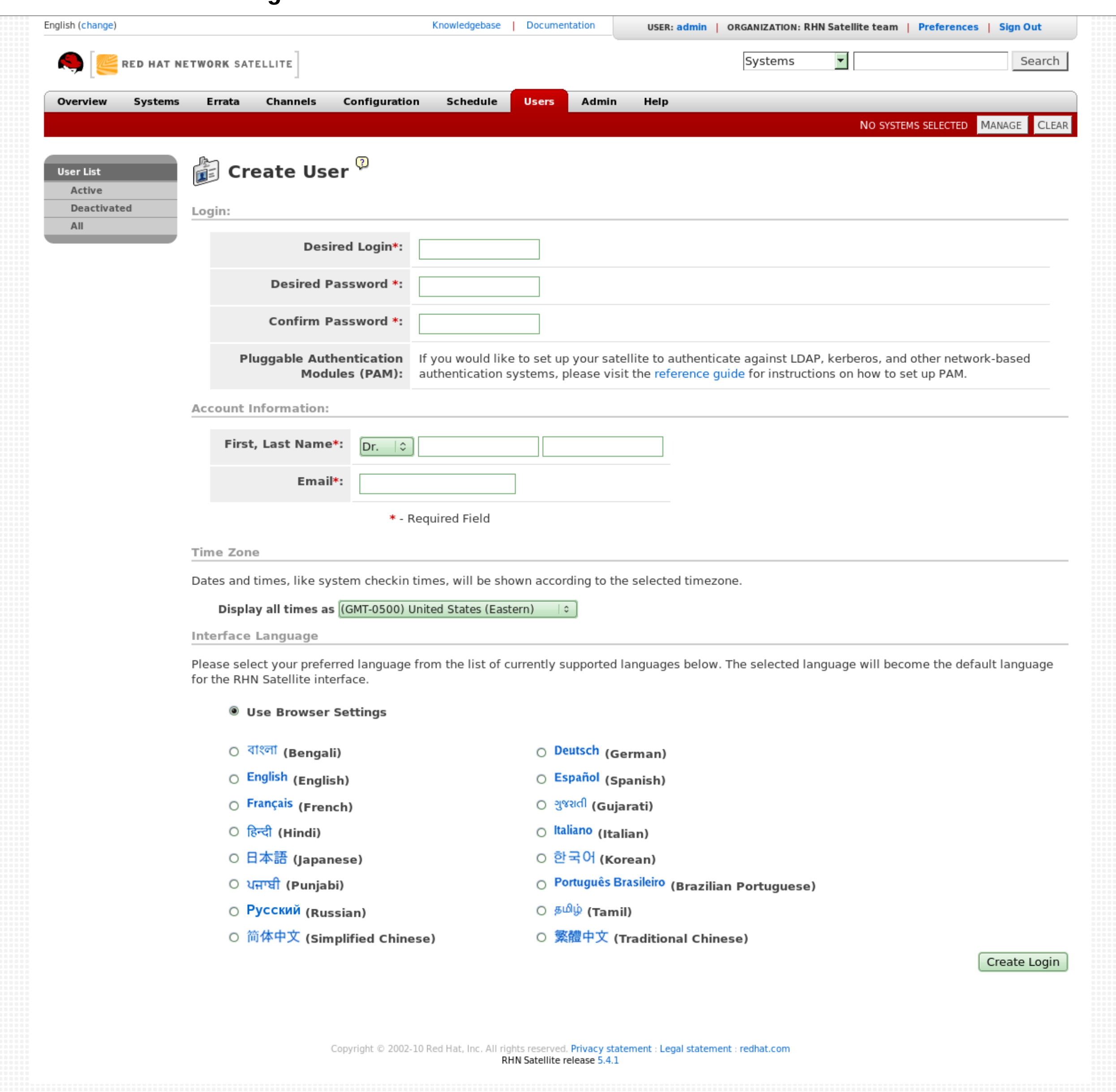
   

   Abbildung 1.1. Die Seite `Benutzer anlegen`

2. Geben Sie im Feld **`Gewünschtes Login`** einen Namen für den Benutzer an. Der Login-Name muss mindestens fünf Zeichen lang sein.

3. Geben Sie im Feld **Gewünschtes Passwort** ein Passwort für den Benutzer an. Wiederholen Sie die Eingabe, um das Passwort zu bestätigen.
4. Geben Sie den Namen des Benutzers im Textfeld **Vor-, Nachname** an und wählen eine Anrede (z.B. Hr., Fr., Dr.) aus dem Drop-Down-Menü.
5. Geben Sie im **E-Mail**-Feld eine E-Mail-Adresse für den Benutzer an.
6. Wählen Sie im Abschnitt **Zeitzone** die passende Zeitzone aus.
7. Wählen Sie im Abschnitt **Sprache der Weboberfläche** die Sprache aus, die für die RHN Satellite Server Oberfläche verwendet werden soll.
8. Klicken Sie auf **Login erstellen**, um den neuen Benutzer zu erstellen. Daraufhin wird eine E-Mail an den Benutzer geschickt (an die E-Mail-Adresse, die während der Erstellung angegeben wurde), um den Benutzer über die Details des neuen Benutzerkontos zu informieren.
9. Nachdem das Benutzerkonto erfolgreich angelegt wurde, werden Sie auf die Seite **Benutzerliste** geleitet. Falls Sie die Berechtigungen und Optionen für den neuen Benutzer anpassen möchten, klicken Sie auf dessen Namen in der Liste. Daraufhin erscheint die **Benutzerdetails**-Seite für diesen Benutzer, von wo aus Sie auf mehreren Unterreitern die gewünschten Änderungen vornehmen können.

Prozedur 1.2. Benutzer deaktivieren

Benutzerkonten können von Administratoren deaktiviert werden, oder Benutzer können ihr eigenes Konto deaktivieren. Es ist nicht möglich, sich mit einem deaktivierten Benutzerkonto bei der RHN Satellite Server Weboberfläche anzumelden oder Aktionen einzuplanen. Jegliche Aktionen, die noch vor der Deaktivierung des Benutzerkontos eingeplant wurden, verbleiben jedoch in der Aktions-Warteschlange, bis sie ausgeführt wurden. Deaktivierte Benutzerkonten können von Administratoren wieder aktiviert werden.

Administratorkonten können erst deaktiviert werden, nachdem die Administratorrolle von diesem Benutzerkonto entfernt wurde.

Um ein Benutzerkonto zu deaktivieren:

1. Wählen Sie den Namen des Benutzers aus der Liste im **Benutzer**-Reiter, um die **Benutzerdetails**-Seite anzuzeigen.
2. Überprüfen Sie, ob der Benutzer ein Satellite-Administrator ist.

   Falls der Benutzer ein Satellite-Administrator ist, entfernen Sie das Häkchen im Auswahlkästchen dieser Rolle und klicken auf **Übernehmen**.

   Falls der Benutzer kein Satellite-Administrator ist, fahren Sie mit dem nächsten Schritt fort.
3. Klicken Sie auf **Benutzer deaktivieren**.

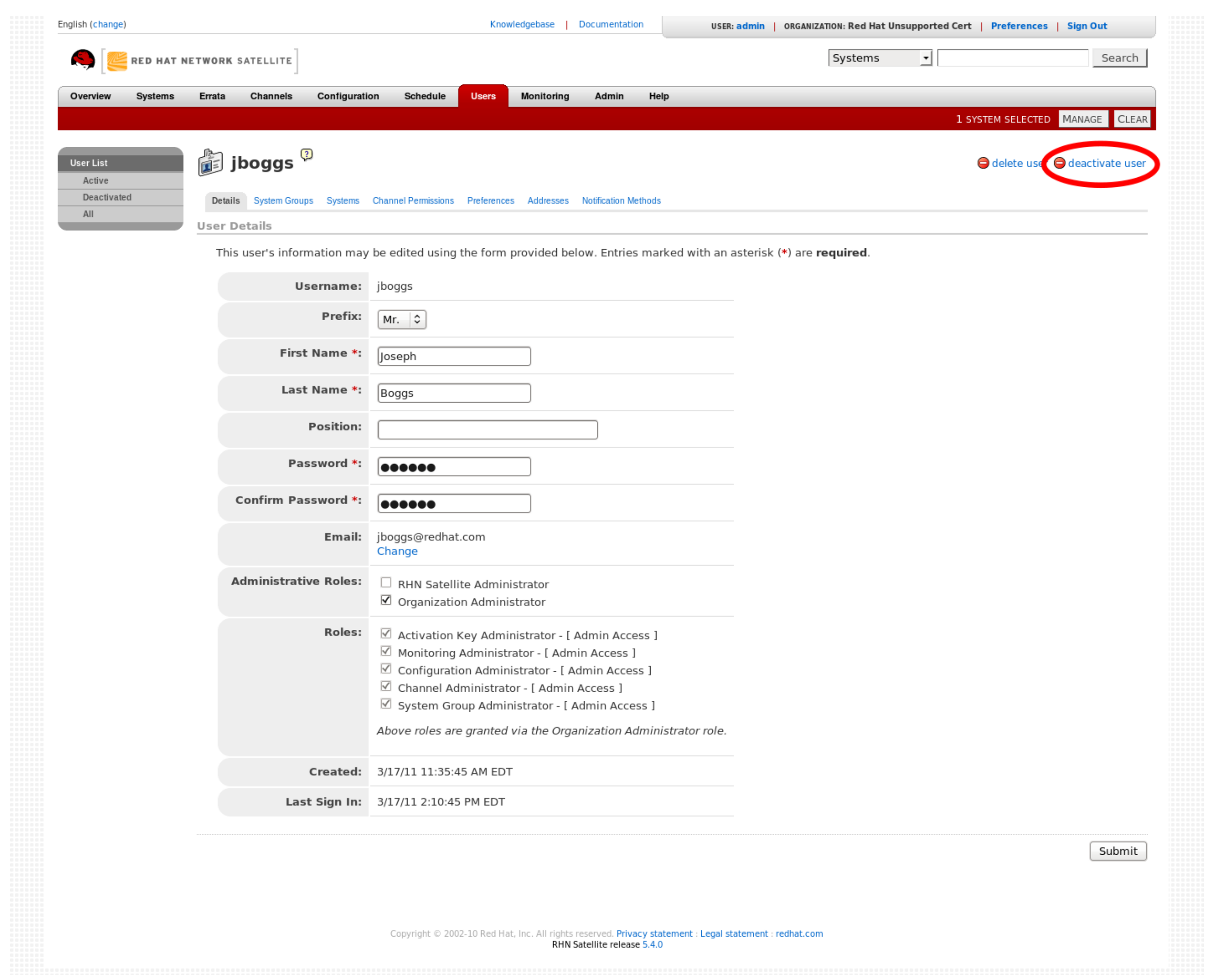


Abbildung 1.2. Benutzer deaktivieren

Sie werden dazu aufgefordert werden, diese Aktion zu bestätigen, indem Sie nochmals die Schaltfläche klicken. Überprüfen Sie die Angaben und klicken zur Bestätigung erneut auf **`Benutzer deaktivieren`**.

4. Sobald das Benutzerkonto erfolgreich deaktiviert wurde, erscheint der Name des Benutzers nicht länger in der **`Aktive Benutzer`** Liste. Klicken Sie auf den **`Deaktiviert`**-Link im **`Benutzerliste`**-Menü, um die deaktivierten Benutzerkonten zu sehen.

5. Um das Benutzerkonto wieder zu aktivieren, markieren Sie in der **`Deaktiviert`**-Liste das Auswahlkästchen neben dem gewünschten Benutzer aus und klicken anschließend auf **`Reaktivieren`**.

Prozedur 1.3. Benutzer löschen

Benutzerkonten können von Administratoren gelöscht werden. Es ist nicht möglich, sich mit einem gelöschten Benutzerkonto bei der RHN Satellite Server Weboberfläche anzumelden oder Aktionen einzuplanen. Gelöschte Benutzerkonten können nicht wieder aktiviert werden.

Administratorkonten können erst gelöscht werden, nachdem die Administratorrolle von diesem Benutzerkonto entfernt wurde.



Warnung

Das Löschen eines Benutzers kann nicht rückgängig gemacht werden; seien Sie deshalb vorsichtig, wenn Sie diese Aktion ausführen. Ziehen Sie ggf. in Betracht, den Benutzer zunächst nur zu deaktivieren, um zu beobachten, welche Folgen ein Löschen für Ihre RHN Satellite Server Infrastruktur hätte.

Um ein Benutzerkonto zu löschen:

1. Wählen Sie den Namen des Benutzers aus der Liste im **`Benutzer`**-Reiter, um die **`Benutzerdetails`**-Seite anzuzeigen.
2. Überprüfen Sie, ob der Benutzer ein Satellite-Administrator ist.

   Falls der Benutzer ein Satellite-Administrator ist, entfernen Sie das Häkchen im Auswahlkästchen dieser Rolle und klicken auf **`Übernehmen`**.

   Falls der Benutzer kein Satellite-Administrator ist, fahren Sie mit dem nächsten Schritt fort.
3. Klicken Sie auf **`Benutzer löschen`**.

English (change) Knowledgebase | Documentation USER: admin | ORGANIZATION: Red Hat Unsupported Cert | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems Search
Overview Systems Errata Channels Configuration Schedule Users Monitoring Admin Help
1 SYSTEM SELECTED MANAGE CLEAR
User List
Active
Deactivated
All
jboggs
delete user deactivate user
Details System Groups Systems Channel Permissions Preferences Addresses Notification Methods
User Details
This user's information may be edited using the form provided below. Entries marked with an asterisk (*) are required.
Username: jboggs
Prefix: Mr.
First Name *: Joseph
Last Name *: Boggs
Position:
Password *: ●●●●●●
Confirm Password *: ●●●●●●
Email: jboggs@redhat.com
Change
Administrative Roles: RHN Satellite Administrator
Organization Administrator
Roles: Activation Key Administrator - [Admin Access]
Monitoring Administrator - [Admin Access]
Configuration Administrator - [Admin Access]
Channel Administrator - [Admin Access]
System Group Administrator - [Admin Access]
Above roles are granted via the Organization Administrator role.
Created: 3/17/11 11:35:45 AM EDT
Last Sign In: 3/17/11 2:10:45 PM EDT
Submit
Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
RHN Satellite release 5.4.0

Abbildung 1.3. Benutzer löschen

Sie werden dazu aufgefordert werden, diese Aktion zu bestätigen, indem Sie nochmals die Schaltfläche klicken. Überprüfen Sie die Angaben und klicken zur Bestätigung erneut auf **`Benutzer löschen`**.

4. Sobald das Benutzerkonto erfolgreich gelöscht wurde, erscheint der Name des Benutzers nicht länger in der **Aktive Benutzer** Liste. Dieser Schritt kann nicht rückgängig gemacht werden.

1.2. Benutzerverwaltung

Benutzerkonten können über den **Benutzer**-Reiter oben in der RHN Satellite Server Navigationsleiste verwaltet werden. Falls Sie die Berechtigungen und Optionen für einen Benutzer anpassen möchten, klicken Sie auf dessen Namen in der Liste. Daraufhin erscheint die **Benutzerdetails**-Seite für diesen Benutzer, von wo aus Sie auf mehreren Unterreitern die gewünschten Änderungen vornehmen können. Ändern Sie die Details des Benutzerkontos wie gewünscht ab und klicken Sie anschließend auf **Übernehmen**.

Benutzerrollen

Benutzerrollen werden dazu verwendet, um Verantwortlichkeiten an Benutzerkonten zu delegieren. Jede Rolle verfügt über eine anderes Maß an Verantwortlichkeiten und Zugriffsrechten.

Um einem Benutzer eine neue Rolle zuzuweisen, markieren Sie das entsprechende Auswahlkästchen auf der **Benutzerdetails**-Seite. Nehmen Sie die gewünschten Änderungen an den Rollen vor und klicken Sie anschließend auf **Übernehmen**.

Folgende Benutzerrollen stehen zur Auswahl:

RHN Satellite-Administrator

Eine besondere Rolle für Satellite-Administrationsaufgaben, wie z.B. zum Erstellen von Organisationen, Verwalten von Subskriptionen und der Konfiguration globaler RHN Satellite Server Einstellungen.

Diese Rolle kann nicht auf der **Benutzerdetails**-Seite zugewiesen werden. Ein Benutzer, der bereits über die RHN Satellite Server Administratorrolle verfügt, kann einem anderen Benutzer diese Rolle unter **Admin** → **Benutzer** zuweisen.

Organisationsadministrator

Führt Verwaltungsfunktionen aus wie z.B. Verwaltung von Benutzern, Systemen und Channels innerhalb des Kontexts seiner Organisation. Organisationsadministratoren wird automatisch administrativer Zugriff auf alle anderen Rollen gewährt, die grau hinterlegt erscheinen.

Aktivierungsschlüssel-Administrator

Führt Aktivierungsschlüssel-Funktionen aus zum Erstellen, Verändern und Löschen von Schlüsseln innerhalb des Accounts.

Channel-Administrator

Bietet umfassenden Zugriff auf die Software-Channels samt zugehöriger Verknüpfungen innerhalb der Organisation. Führt Funktionen aus, um z.B. Channels global subskribierbar zu machen, neue Channels zu erstellen und Pakete innerhalb der Channels zu verwalten.

Konfigurations-Administrator

Verfügt über umfassenden Zugriff auf die Konfigurations-Channels samt zugehöriger Verknüpfungen innerhalb der Organisation. Führt Konfigurationsfunktionen aus zur Channel- und Dateiverwaltung in der Organisation.

`Monitoring-Administrator`
: Führt Funktionen zum Einplanen von Probes aus und überwacht andere Monitoring-Infrastruktur. Diese Rolle steht nur auf RHN Satellite Servern mit aktiviertem Monitoring zur Verfügung.

`Systemgruppen-Administrator`
: Diese Rolle verfügt über umfassende Rechte über jene Systeme und Systemgruppen, auf die ihr Zugriff gewährt wurde. Führt administrative Funktionen aus wie z.B. Erstellen neuer Systemgruppen, Löschen zugewiesener Systemgruppen, Hinzufügen von Systemen zu Gruppen und Verwaltung des Benutzerzugriffs auf Gruppen.

Satellite-Administratoren können zwar einem anderen Benutzer die Satellite-Administratorrechte entziehen, allerdings ist es nicht möglich, dem letzten verbleibenden Satellite-Administrator diese Rechte zu entziehen. Es muss zu jeder Zeit mindestens ein Satellite-Administrator existieren. Es ist auch möglich, dass ein Satellite-Administrator sich selbst die Satellite-Administratorrechte entzieht, sofern er nicht der letzte verbleibende Satellite-Administrator ist.

Kapitel 2. Automatische Synchronisation

Das manuelle Synchronisieren des RHN Satellite Server Repositorys mit dem Red Hat Network kann eine mühselige Aufgabe sein. Die Synchronisation kann jedoch automatisiert werden, so dass sie zu Nebenzeiten durchgeführt werden kann wie z.B. am späten Abend oder am frühen Morgen, um die Auslastung besser zu verteilen und eine schnelle Synchronisation zu gewährleisten. Die Synchronisierung sollte für eine optimale Leistung zufällig erfolgen. Am effektivsten ist die Automatisierung der Synchronisation mithilfe von **cron**.

Prozedur 2.1. Automatisieren der Synchronisation

1. Wechseln Sie zum Root-Benutzer und öffnen Sie **crontab** in einem Texteditor:

   ```
   crontab -e
   ```

   Anmerkung

   crontab wird standardmäßig in vi geöffnet. Um dieses Verhalten zu ändern, setzen Sie die **EDITOR**-Variable auf den Namen des stattdessen gewünschten Texteditors.

2. Verwenden Sie in der **crontab**-Datei die ersten fünf Felder (Minute, Stunde, Tag, Monat und Wochentag), um den Zeitpunkt der Synchronisation festzulegen. Um eine zufällige Synchronisation zu erreichen, verwenden Sie den folgenden Eintrag:

   ```
   0 1 * * * perl -le 'sleep rand 9000' && satellite-sync --email >/dev/null
   2>1
   ```

   Dieser **crontab**-Eintrag wird den Synchronisations-Job zufällig zwischen 01:00 und 03:30 ausführen. Ausgaben von **cron** auf ***stdout*** und ***stderr*** werden verworfen, um doppelte Meldungen von **satellite-sync** zu vermeiden. Je nach Bedarf können noch weitere Optionen angegeben werden.

3. Um die **crontab**-Datei zu speichern, beenden Sie einfach den Texteditor. Die neuen **cron**-Regeln werden daraufhin sofort wirksam.

Kapitel 3. Datensicherung und Wiederherstellung

Dieses Kapitel erläutert Methoden zur Sicherung, Überprüfung und Wiederherstellung eines Satellite-Systems.

Die Datensicherung sollte entweder jede Nacht oder jede Woche erfolgen, abhängig von der Menge der gespeicherten Daten, und von der Menge an Daten, die Sie im Falle eines Systemausfalls gewillt sind zu verlieren.

Es wird empfohlen, dass Sie die Datenbanksicherungen während planmäßigen Wartungsphasen des RHN Satellite Servers durchführen, da während der Datensicherung keiner der Dienste für Website- und Client-Verbindungen zur Verfügung stehen.

3.1. Datensicherung

Prozedur 3.1. Sichern der eingebetteten Datenbank

1. Stoppen Sie den RHN Satellite Server mithilfe des **`stop`**-Befehls:

   ```
   rhn-satellite stop
   ```

2. Wechseln Sie zum Oracle-Benutzer und erstellen Sie die Sicherungskopie mithilfe des **`db-control`**-Dienstprogramms:

   ```
   su - oracle
   db-control backup [directory]
   ```

   Ersetzen Sie ***`directory`*** durch den absoluten Pfad zu dem Speicherort, an dem Sie eine Sicherungskopie Ihrer Datenbank anlegen möchten. Dieser Vorgang nimmt einige Minuten in Anspruch.

3. Wechseln Sie zurück zum Root-Benutzer und starten Sie den Satellite:

   ```
   exit
   rhn-satellite start
   ```

4. Wechseln Sie zum Oracle-Benutzer und überprüfen Sie mithilfe der **`examine`**-Option des **`db-control`**-Befehls den Zeitstempel der Sicherungskopie und ob möglicherweise Dateien fehlen:

   ```
   su - oracle
   db-control examine [directory]
   ```

   Sie können auch die **`verify`**-Option von **`db-control`** verwenden, um eine gründliche Untersuchung durchzuführen, einschließlich Prüfung der md5-Prüfsumme jeder einzelnen gesicherten Datei:

   ```
   db-control verify [directory]
   ```

   Ist diese Überprüfung erfolgreich, ist es sicher, die Inhalte von ***`directory`*** zur Wiederherstellung der Datenbank zu verwenden.



Anmerkung

Auch Benutzer von externen Datenbanken sollten regelmäßig ihre Daten sichern. Setzen Sie sich mit dem Administrator Ihrer externen Datenbank in Verbindung, um mehr über die unterstützten Verfahren zur Datensicherung zu erfahren.

Sichern von Systemdateien

Zusätzlich zur Datenbank sollten auch eine Reihe von Systemdateien und -verzeichnissen gesichert werden. Nachfolgend sehen Sie eine Liste derjenigen Dateien und Verzeichnisse, die gesichert werden sollten:

- **/etc/sysconfig/rhn/**
- **/etc/rhn/**
- **/etc/sudoers**
- **/etc/tnsnames.ora**
- **/var/www/html/pub/**
- **/var/satellite/redhat/[0-9]*/** (Dies ist der Speicherort für jegliche angepasste RPMs)
- **/root/.gnupg/**
- **/root/ssl-build/**
- **/etc/dhcpd.conf**
- **/etc/httpd/**
- **/tftpboot/**
- **/var/lib/cobbler/**
- **/var/lib/nocpulse/**
- **/var/lib/rhn/kickstarts/**
- **/var/www/cobbler/**

Sichern Sie nach Möglichkeit auch **/var/satellite/**. Dies ist eine Kopie des Red Hat RPM-Repositorys und erspart Ihnen einen umfangreichen Download, falls Sie nach einem Ausfall das System wiederherstellen müssen. Es kann mithilfe des **satellite-sync**-Tools regeneriert werden. Falls Sie einen nicht verbundenen Satellite nutzen, muss **/var/satellite/** gesichert werden, damit eine Wiederherstellung nach Ausfall überhaupt möglich ist.

Wenn Sie nur die oben genannten Dateien und Verzeichnisse sichern, müssten Sie zur Wiederherstellung die RHN Satellite Server ISO-RPMs neu installieren und den Satellite erneut registrieren. Zusätzlich müssten Red Hat Pakete mithilfe des **satellite-sync**-Tools synchronisiert werden und das **/root/ssl-build/rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm** Paket müsste installiert werden. Alternativ können Sie den RHN Satellite Server neu installieren, ohne ihn erneut zu registrieren. Überspringen Sie dazu während der Installation die Red Hat Network Registrierung und die Abschnitte zur Generierung von SSL-Zertifikaten.

Die umfassendste Methode ist die vollständige Sicherung der gesamten Maschine. Dies verkürzt zwar ggf. die zum Download und zur Neuinstallation nötige Zeit, erfordert jedoch mehr Festplattenplatz und verlängert die zur Datensicherung nötige Zeit.

3.2. Wiederherstellung von der Sicherungskopie

Mithilfe der Red Hat Network Database Control wird die eingebettete Datenbank von der Sicherungskopie wiederhergestellt.

Prozedur 3.2. Wiederherstellung der eingebetteten Datenbank von der Sicherungskopie

1. Stoppen Sie den RHN Satellite Server mithilfe des **stop**-Befehls:

```
rhn-satellite stop
```

2. Wechseln Sie zum Oracle-Benutzer und stellen mithilfe des **db-control**-Dienstprogramms wieder von der Sicherungskopie her:

```
su - oracle
db-control restore [directory]
```

   Ersetzen Sie ***directory*** durch den absoluten Pfad zu dem Speicherort, der die Sicherungskopie Ihrer Datenbank enthält. Dieser Vorgang überprüft die Inhalte der Sicherungskopie vor der Wiederherstellung, weshalb er einige Minuten in Anspruch nimmt.

3. Wechseln Sie zurück zum Root-Benutzer und starten Sie den Satellite:

```
exit
rhn-satellite start
```

4. Unabhängig davon, ob Sie eine externe oder eine eingebettete Datenbank wiederherstellen, müssen Sie zur Wiederherstellung des Satellites von den gesicherten Daten den folgenden Befehl ausführen, um die Neuerstellung von Suchindizes einzuplanen, sobald der **rhn-search**-Dienst das nächste Mal gestartet wird:

```
/etc/init.d/rhn-search cleanindex
```

3.3. Automatisierte Datensicherung

Die Datensicherung kann automatisiert werden, damit diese zu Nebenzeiten durchgeführt wird, beispielsweise am späten Abend oder am frühen Morgen. Dadurch wird zudem sichergestellt, dass die Datensicherung regelmäßig erfolgt und nicht vergessen wird. Am effektivsten ist die Automatisierung der Synchronisation mithilfe von **cron**.

Prozedur 3.3. Automatisierung der Datensicherung

Erstellen Sie eine neue Datei namens **backup-db.sh**, die das folgende Skript enthält. Dieses Skript wird den Satellite stoppen, eine Datenbanksicherung durchführen, und den Satellite nach Abschluss wieder starten:

```
#!/bin/bash
{
/usr/sbin/rhn-satellite stop
su - oracle -c'
d=db-backup-$(date "+%F");
mkdir -p /tmp/$d;
db-control backup /tmp/$d
';
/usr/sbin/rhn-satellite start
} &> /dev/null
```

1. Erstellen Sie eine neue Datei namens **`move-files.sh`**, die das folgende Skript enthält. Dieses Skript nutzt **`rsync`**, um die gesicherten Daten in ein Verzeichnis zu verlegen:

   ```
   #!/bin/bash
   rsync -avz /tmp/db-backup-$(date "+%F") [destination] &> /dev/null
   ```

   Ersetzen Sie dabei ***`[destination]`*** durch den Pfad zum Sicherungsverzeichnis.

   Alternativ nutzt das folgende Skript für den gleichen Zweck **`scp`**:

   ```
   #!/bin/bash
   scp -r /tmp/db-backup-$(date "+%F") [destination] &> /dev/null
   ```

2. Wechseln Sie zum Root-Benutzer und öffnen Sie **`crontab`** in einem Texteditor:

   ```
   crontab -e
   ```

   Anmerkung

   `crontab` wird standardmäßig in vi geöffnet. Um dieses Verhalten zu ändern, setzen Sie die **`EDITOR`**-Variable auf den Namen des stattdessen gewünschten Texteditors.

3. Verwenden Sie in der **`crontab`**-Datei die ersten fünf Felder (Minute, Stunde, Tag, Monat und Wochentag), um den Zeitpunkt zum Ausführen der Skripte festzulegen:

   ```
   0 3 * * * backup-db.sh
   0 6 * * * move-files.sh
   ```

   Dieser **`crontab`**-Eintrag wird die Datensicherung um 03:00 durchführen und die gesicherten Daten um 06:00 verschieben. Je nach Bedarf können noch weitere Optionen angegeben werden. Sie können darüber hinaus noch ein Skript zur Bereinigung einfügen, um ältere Sicherungsverzeichnisse zu löschen und so zu vermeiden, dass sich der Sicherungsdatenträger allmählich anfüllt.

4. Um die **`crontab`**-Datei zu speichern, beenden Sie einfach den Texteditor. Die neuen **`cron`**-Regeln werden daraufhin sofort wirksam.

Kapitel 4. Klonen einer Maschine

Der Befehl **`spacewalk-clone-by-date`** ermöglicht es RHN Satellite Kunden, angepasste, geklonte Red Hat Enterprise Linux Channels zu erstellen, basierend auf dem Datum, an dem das Erratum für das Red Hat Enterprise Linux System ausgegeben wurde.

4.1. Funktionsumfang

Der Befehl **`spacewalk-clone-by-date`** bietet folgende Funktionen:

- Klonen des Channels in dem Zustand, in dem er sich an einem bestimmten Datum befand
- Automatisieren des Klonvorgangs durch Skripte und Vorlagendateien
- Entfernen oder Sperren von Paketen in Channels
- Auflösen von Paketabhängigkeiten innerhalb der über- und untergeordneten Channels
- Filtern und Anwenden bestimmter Errata, während andere ignoriert werden. Beispielsweise nur Anwenden von Sicherheits-Errata, während Fehlerbehebungen und Erweiterungen ignoriert werden.



Anmerkung

Der Befehl **`spacewalk-clone-by-date`** muss als *Root-Benutzer* ausgeführt werden und der **`username`** muss entweder ein Organisationsadministrator oder Channel-Administrator sein.

4.2. Befehlszeilenoptionen

Tabelle 4.1. Verfügbare Befehlszeilenoptionen

Optionen	Definition
-h, --help	Zeigt die Hilfedatei.
-c CONFIG, --config=CONFIG	Ermöglicht dem Benutzer die Angabe einer Konfigurationsdatei, in der alle Optionen spezifiziert sind. Jegliche Optionen, die auf der Befehlszeile angegeben werden können, können in dieser Konfigurationsdatei spezifiziert werden. Die Konfigurationsdatei ermöglicht es Benutzern, eine komplexe Liste mit zu klonenden Channels anzulegen und die genauen Befehle für spätere Wiederverwendung zu speichern.
-u USERNAME, --username=USERNAME	Spezifiziert den Benutzernamen zur Anmeldung beim Satellite.
-p PASSWORD, --password=PASSWORD	Spezifiziert das Passwort für den Benutzernamen
-s SERVER, --server=SERVER	Server-URL für API-Verbindungen. Standardmäßig https://localhost/rpc/api
-l CHANNELS, --channels=CHANNELS	Spezifiziert die zu klonenden Channels. Channel-Labels müssen in originalen Klonpaaren angegeben werden. Vergewissern Sie sich, bei der Angabe von Klonpaaren diese durch Leerzeichen voneinander zu trennen. Zusätzliche Channels können spezifiziert werden, indem Sie die --channels Option mehrmals verwenden.
-b BLACKLIST, --blacklist=BLACKLIST	Kommagetrennte Liste mit Paketnamen (oder regulären Ausdrücken), die vom geklonten Errata ausgeschlossen werden sollen (Nur hinzugefügte Pakete werden berücksichtigt).
-r REMOVELIST, --removelist=REMOVELIST	Kommagetrennte Liste mit Paketnamen (oder regulären Ausdrücken), die vom Ziel-Channel entfernt werden sollen (Alle Pakete können entfernt werden).
-d TO_DATE, --to_date=TO_DATE	Klont Errata bis zum angegebenen Datum (YYYY-MM-DD). Ermöglicht es dem Benutzer, die originalen Pakete sowie jegliche spezifische Errata seit Erstellung des originalen Channels bis zum angegebenen Datum (**`TO_DATE`**-Parameter) zu klonen. So kann ein zeitbasierter Snapshot des Channels für den durch TO_DATE angegebenen Zeitraum erhalten werden.
-y, --assumeyes	Nimmt "Yes" an für jegliche Bestätigungsfragen. Dies wird für das

	automatisierte Klonen verwendet.
-m, --sample-config	Zeigt eine vollständige Beispiel-Konfigurationsdatei an und beendet.
-k, --skip_depsolve	Überspringt das Auflösen von Abhängigkeiten (nicht empfohlen)
-v, --validate	"repoclosure" auf der Gruppe der angegebenen Repositorys ausführen.
-g, --background	Klont das Erratum im Hintergrund. Kehrt früher zur Eingabeaufforderung zurück, noch bevor das Klonen beendet wird.
-o, --security_only	Nur Sicherheits-Errata (und deren Abhängigkeiten) klonen. Dieser Befehl kann zusammen mit dem **`--to_date`**-Befehl verwendet werden, um nur Sicherheits-Errata zu klonen, die vor oder an einem bestimmten Datum veröffentlicht wurden.

4.3. Beispielverwendung

Das nachstehende Beispiel klont den **`rhel-i386-server-5`**-Channel mit Stand 1. Januar 2012 in den Channel namens my-clone-RHEL-5.

```
# spacewalk-clone-by-date --username=your_username --password=your_password --
server=satellite_server_url --channels=rhel-i386-server-5 my-clone-RHEL-5 --
to_date=2012-01-01
```

Das nachstehende Beispiel klont nur Sicherheits-Errata, die an oder vor dem 1. Januar 2012 veröffentlicht wurden und ignoriert dabei jegliche Kernel-Aktualisierungen oder vim-erweiterte Pakete. Der Befehl führt den Klonvorgang zudem im Hintergrund auf dem Satellite aus.

```
# spacewalk-clone-by-date --username=your_username --password=your_password --
server=satellite_server_url --channels=rhel-i386-server-5 my-clone-RHEL-5 --
to_date=2012-01-01 --security_only --background --blacklist=kernel,vim-extended --
assumeyes
```

Kapitel 5. Monitoring

RHN Satellite Server beinhaltet viele verschiedene Komponenten, von denen viele überwacht werden können. Dieses Kapitel zeigt Wege auf, wie Sie Operationen zur Überwachung ("Monitoring") einer Vielzahl verschiedener Bereiche des Systems durchführen können.

Prozedur 5.1. Überwachung des Tabellenraums

1. In Oracle-Datenbanken ist es wichtig, regelmäßig zu überprüfen, ob der Tabellenraum noch genügend freien Platz hat. Wechseln Sie dazu zum ***Oracle***-Benutzer und führen den **db-control report** Befehl aus:

   ```
   su - oracle
   db-control report
   Tablespace     Size  Used Avail  Use%
   DATA_TBS       4.8G 3.9G  996M   80%
   SYSTEM         250M 116M  133M   46%
   TOOLS          128M 3M    124M   2%
   UNDO_TBS       1000M 61M  938M   6%
   USERS          128M 64K   127M   0%
   ```

2. Falls ein Tabellenraum zu voll wird, kann er erweitert werden, indem Sie den Befehl **db-control extend** mit dem Namen des zu erweiternden Tabellenraums ausführen:

   ```
   db-control extend tablespace
   ```

Prozedur 5.2. Überwachung von RHN Satellite Server Prozessen

- Überprüfen Sie, dass Satellite-Prozesse ausgeführt werden, indem Sie den **rhn-satellite status**-Befehl ausführen:

  ```
  rhn-satellite status
  ```

Kapitel 6. OpenSCAP

SCAP ist eine standardisierte Lösung zur Konformitätsprüfung (Compliance) für Linux-Infrastrukturen der Unternehmensklasse. Es besteht aus einer Reihe von Spezifikationen, die vom National Institute of Standards and Technology (NIST) gepflegt werden und der Wahrung der Systemsicherheit von Unternehmenssystemen dienen.

In RHN Satellite Server 5.5 wird SCAP durch die **OpenSCAP**-Applikation implementiert. **OpenSCAP** ist ein Auditing-Tool, das das Extensible Configuration Checklist Description Format (XCCDF) verwendet. XCCDF ist ein standardisiertes Format für Prüflisteninhalte und definiert Sicherheitsprüflisten. Es kombiniert zudem andere Spezifikationen wie z.B. CPE, CCE und OVAL, um eine SCAP-Prüfliste zu erstellen, die von SCAP-validierten Produkten verarbeitet werden kann.

6.1. OpenSCAP-Funktionsumfang

OpenSCAP prüft anhand der vom Red Hat Security Response Team (SRT) bereitgestellten Inhalte, ob Patches vorhanden sind, prüft die Konfigurationseinstellungen zur Systemsicherheit und untersucht Systeme auf Hinweise zur Gefährdung anhand von Regeln basierend auf Standards/Spezifikationen.

Es gibt zwei Voraussetzungen, um OpenSCAP effektiv einzusetzen:

- Ein Tool zum Prüfen, ob ein System einem Standard entspricht

  RHN Satellite Server hat ab Version 5.5 OpenSCAP als Auditing-Feature integriert. Es erlaubt Ihnen das Einplanen und Ansehen von Konformitätsscans für das System über die Weboberfläche.

- SCAP-Inhalt

  SCAP-Inhalte können von Grund auf neu erstellt werden, sofern Sie Kenntnisse von mindestens XCCDF oder OVAL haben. Alternativ gibt es eine andere Möglichkeit: XCCDF-Inhalte werden häufig online unter Open-Source-Lizenzen veröffentlicht; unter Umständen können Sie diese Inhalte auf Ihre Bedürfnisse anpassen.

  Anmerkung

  Red Hat unterstützt die Verwendung von Vorlagen zur Prüfung Ihres Systems. Allerdings wird die benutzerdefinierte Anpassung dieser Vorlagen nicht unterstützt.

  Ein paar Beispiele für diese Gruppen:

  - The United States Government Configuration Baseline (USGCB) für RHEL5 Desktop — Offizieller SCAP-Inhalt für Arbeitsplatzrechner in US-amerikanischen Bundesbehörden, der von NIST in Zusammenarbeit mit Red Hat, Inc. und dem United States Department of Defense (DoD) unter Verwendung von OVAL entwickelt wurde.
  - Inhalte von der Community
    - SCAP Sicherheitshandbuch für RHEL6 — Aktiver Inhalt aus der Community, basierend auf den USGCB-Anforderungen und verbreiteten Richtlinien; enthält Profile für Arbeitsplatzrecher, Server und FTP-Server.
    - OpenSCAP-Inhalte für RHEL6 — Das **openscap-content**-Paket aus dem Red Hat Enterprise Linux 6 Optional Channel stellt ebenfalls Hilfestellung zu Standardinhalten für Red Hat Enterprise Linux 6 Systeme mittels einer Vorlage bereit.

Da SCAP zur Wahrung der Systemsicherheit konzipiert wurde, unterliegen die verwendeten Standards kontinuierlichen Änderungen, um mit veränderten Anforderungen der Community und der Unternehmenskunden Schritt zu halten. Neue Spezifikationen werden vom SCAP Release Cycle des NISTs gesteuert, um einen konsistenten und wiederholbaren Revisionszyklus zu gewährleisten.

6.2. OpenSCAP in RHN Satellite

6.2.1. Voraussetzungen

Paketvoraussetzungen

SCAP erfordert die folgenden Pakete:

- Für den Server: RHN Satellite 5.5
- Für den Client: **spacewalk-oscap**-Paket (verfügbar vom RHN Tools Sub-Channel)

Berechtigungsvoraussetzungen

Eine Management-Berechtigung ist erforderlich, um Scans einzuplanen.

Sonstige Voraussetzungen

Für den Client: Verteilen der XCCDF-Inhalte an Client-Rechner

Sie können die XCCDF-Inhalte mit einer der folgenden Methoden auf die Client-Rechner verteilen:

- Herkömmliche Methoden (CD, USB, nfs, scp, ftp)
- Satellite-Skripte
- RPMs

  Angepasste RPMs sind die empfohlene Methode zum Verteilen von SCAP-Inhalten auf andere Rechner. RPM-Pakete können signiert und verifiziert werden, um deren Integrität sicherzustellen. Installation, Entfernung und Verifizierung von RPM-Paketen kann von der Benutzeroberfläche aus gehandhabt werden.

6.2.2. Durchführen von Prüfscans

Die **OpenSCAP**-Integration im RHN Satellite Server ermöglicht es Ihnen, Prüfscans auf Client-Systemen durchzuführen. Dieser Abschnitt erläutert die beiden verfügbaren Methoden.

Prozedur 6.1. Scans über die Weboberfläche

Führen Sie die folgenden Schritte aus, um einen Scan über die Satellite-Weboberfläche durchzuführen:

1. Melden Sie sich auf der Satellite-Weboberfläche an.
2. Klicken Sie auf **Systeme** → **Zielsystem**.
3. Klicken Sie auf **Prüfen** → **Plan**
4. Füllen Sie das ***Neuen XCCDF-Scan planen*** Formular aus:
   - Befehlszeilenparameter: In diesem Feld können zusätzliche Parameter für das oscap-Tool angegeben werden. Nur zwei Befehlszeilenparameter sind zulässig, und zwar:

     --profile PROFILE — Wählt ein bestimmtes Profil aus dem XCCDF-Dokument. Profile sind in der XCCDF-XML-Datei festgelegt und können mithilfe des ***Profile id***-Tags geprüft werden. Zum Beispiel:

     ```
     Profile id="RHEL6-Default"
     ```



Anmerkung

Bestimmte Versionen von OpenSCAP benötigen den --profile Befehlszeilenparameter, andernfalls wird der Scan fehlschlagen.

--skip-valid — Ein-/Ausgabedateien nicht validieren. Benutzer mit ordnungsgemäßem XCCDF-Inhalt können mithilfe dieser Option die Dateivalidierung überspringen.

Falls kein Befehlszeilenparameter angegeben ist, wird das Standardprofil verwendet.

- Pfad zum XCCDF-Dokument: Dies ist ein erforderliches Feld. Der ***path***-Parameter verweist auf den Speicherort der Inhalte auf dem Client-System. Zum Beispiel: **/usr/local/scap/dist_rhel6_scap-rhel6-oval.xml**



Warnung

Der XCCDF-Inhalt wird validiert, bevor er auf dem entfernten System ausgeführt wird. Werden ungültige Parameter angegeben, so kann die Ausführung oder Validierung von spacewalk-oscap fehlschlagen. Aus Sicherheitsgründen akzeptiert der 'osccap xccdf eval' Befehl nur ein eingeschränkte Reihe von Parametern.

5. Führen Sie **rhn_check** aus um sicherzugehen, dass die Aktion vom Client-System übernommen wird.

```
rhn_check -vv
```



Anmerkung

Alternativ, falls **rhnsd** oder **osad** auf dem Client-System laufen, so wird die Aktion von diesen Diensten übernommen. Um sicherzustellen, dass diese Dienste laufen:

```
service rhnsd start
```

oder

```
service osad start
```

Zum Ansehen der Scanergebnisse werfen Sie bitte einen Blick auf Abschnitt 6.2.3, „Anzeigen von SCAP-Ergebnissen“.

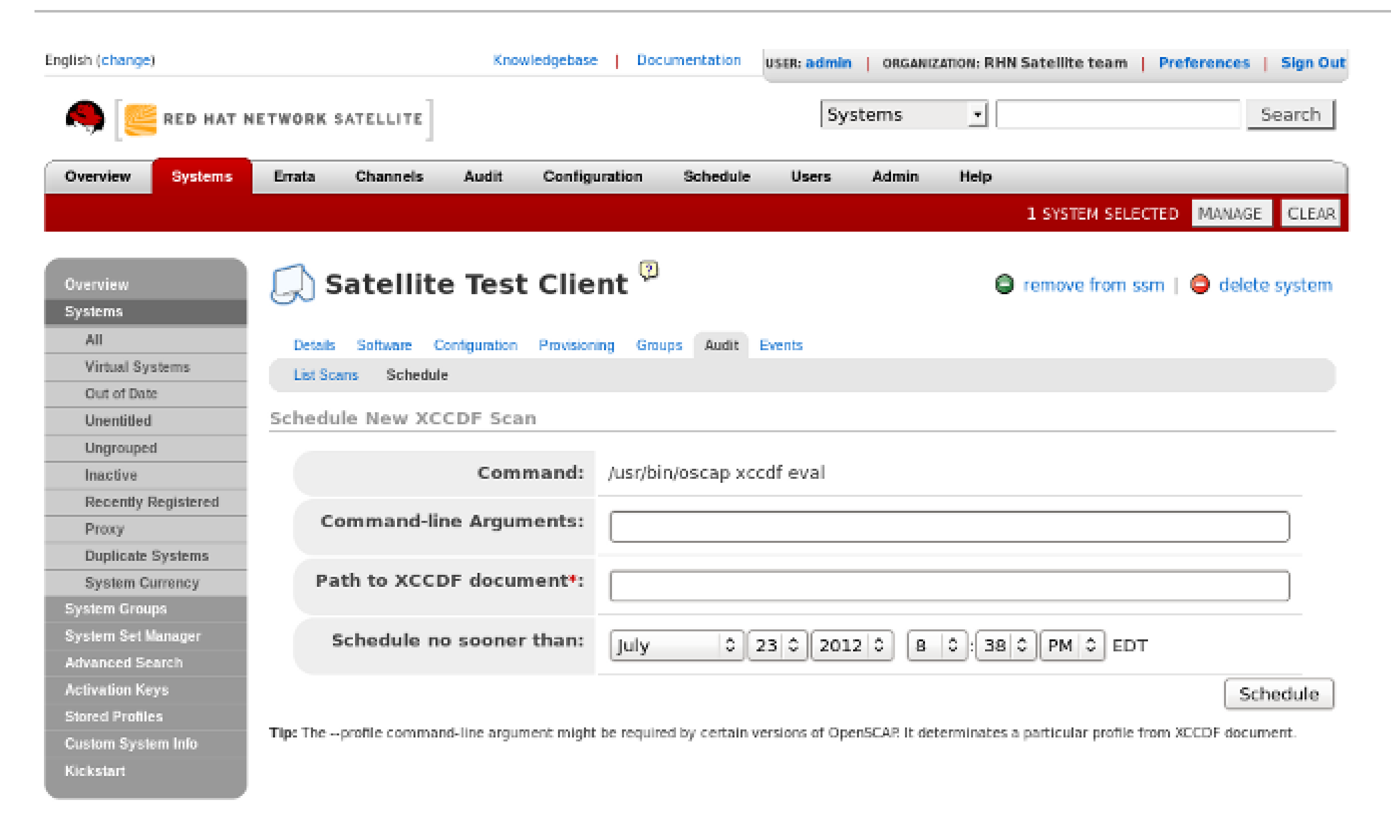


Abbildung 6.1. Einplanen eines Scans per Weboberfläche

Prozedur 6.2. Scans per API

Um einen Prüfscan per API durchzuführen:

1. Wählen Sie ein vorhandenes Skript oder erstellen Sie ein Skript, um einen Systemscan über die Frontend-API **`system.scap.scheduleXccdfScan`** einzuplanen.

   Beispielskript:

   ```
   #!/usr/bin/python
   client = xmlrpclib.Server('https://spacewalk.example.com/rpc/api')
   key = client.auth.login('username', 'password')
   client.system.scap.scheduleXccdfScan(key, 1000010001,
       '/usr/local/share/scap/usgcb-rhel5desktop-xccdf.xml',
       '--profile united_states_government_configuration_baseline')
   ```

   Wobei gilt:

   - 1000010001 ist die ***`System-ID (sid)`***.
   - **`/usr/local/share/scap/usgcb-rhel5desktop-xccdf.xml`** ist der Pfadparameter, der auf den Speicherort des Inhalts auf dem Client-System verweist. In diesem Fall befindet sich der USGSB-Inhalt im **`/usr/local/share/scap`**-Verzeichnis.
   - **`--profile united_states_government_configuration_baseline`** steht für den zusätzlichen Parameter für das oscap-Tool. In diesem Fall wird USCFGB verwendet.

2. Führen Sie das Skript auf der Befehlszeile eines beliebigen Systems aus. Das System benötigt die entsprechenden python- und xmlrpc-Bibliotheken.
3. Führen Sie **`rhn_check`** aus um sicherzugehen, dass die Aktion vom Client-System übernommen wird.

```
rhn_check -vv
```



Anmerkung

Alternativ, falls **rhnsd** oder **osad** auf dem Client-System laufen, so wird die Aktion von diesen Diensten übernommen. Um sicherzustellen, dass diese Dienste laufen:

```
service rhnsd start
```

oder

```
service osad start
```

6.2.3. Anzeigen von SCAP-Ergebnissen

Es gibt drei Methoden zum Anzeigen der Ergebnisse von abgeschlossenen Scans:

- Per Weboberfläche. Sobald die Aktion ausgeführt wurde, sollten die Ergebnisse auf dem **Prüfen**-Reiter des Systems erscheinen. Diese Seite wird in Abschnitt 6.2.4, „OpenSCAP Satellite-Seiten“ erläutert.
- Per API-Funktionen in Handler **system.scap**.
- Per **spacewalk-reports**-Tool des Satellites durch Ausführen der folgenden Befehle:

```
# /usr/bin/spacewalk-reports system-history-scap
# /usr/bin/spacewalk-reports scap-scan
# /usr/bin/spacewalk-reports scap-scan-results
```

6.2.4. OpenSCAP Satellite-Seiten

Die folgenden Abschnitte beschreiben die Reiter auf der RHN Satellite Weboberfläche, die OpenSCAP umfassen.

6.2.4.1. Prüfen

Der **Prüfen**-Reiter auf der oberen Navigationsleiste ist die umfassende Seite für die OpenSCAP-Funltionalität in RHN Satellite Server 5.5. Klicken Sie auf diesen Reiter, um abgeschlossene OpenSCAP-Scans anzusehen, zu durchsuchen und zu vergleichen.

Prüfen → Alle Scans

Alle Scans ist die Standardseite, die beim Klick auf den **Prüfen**-Reiter angezeigt wird. Diese Seite zeigt alle abgeschlossenen OpenSCAP-Scans, die der Benutzer zu sehen berechtigt ist. Die Berechtigungen für die Scans werden aus den Systemberechtigungen abgeleitet.

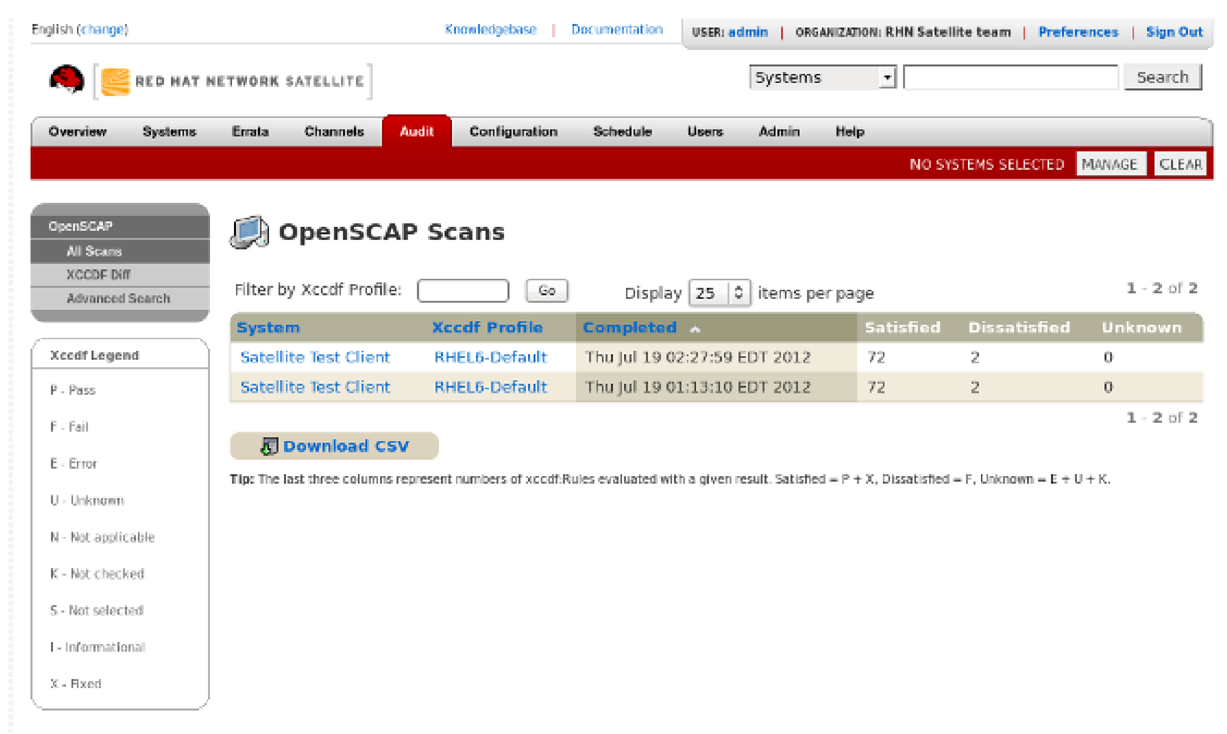


Abbildung 6.2. Prüfen ⇒ Alle Scans

Für jeden Scan werden die folgenden Informationen angezeigt:

System
: Das Zielsystem des Scans

XCCDF-Profil
: Das evaluierte Profil

Abgeschlossen
: Zeit der Fertigstellung

Erfüllt
: Die Anzahl der Regeln, die erfüllt bzw. erfolgreich waren. Eine Regel wird als erfüllt betrachtet, wenn das Ergebnis der Evaluierung entweder "Erfolgreich" oder "Behoben" ist.

Nicht erfüllt
: Die Anzahl der Regeln, die nicht erfüllt wurden bzw. fehlgeschlagen sind. Eine Regel wird als nicht erfüllt betrachtet, wenn das Ergebnis der Evaluierung "Fehlgeschlagen" ist.

Unbekannt
: Die Anzahl der Regeln, die nicht evaluiert werden konnten. Eine Regel wird als "unbekannt" betrachtet, wenn das Ergebnis der Evaluierung "Fehler", "Unbekannt" oder "Nicht geprüft" ist.

Die Evaluierung von XCCDF-Regeln kann auch Status wie **Informationell**, **Nicht zutreffend** oder **Nicht ausgewählt** zurückgeben. In diesen Fällen ist die jeweilige Regel in den Statistiken auf dieser Seite nicht enthalten. Siehe **Systemdetails** → **Prüfen** für Informationen über diese Regeln.

Prüfen → XCCDF Diff

XCCDF Diff ist eine Applikation, die den Vergleich von zwei XCCDF-Scans grafisch veranschaulicht. Sie zeigt Metadaten für zwei Scans sowie die Liste der Ergebnisse.

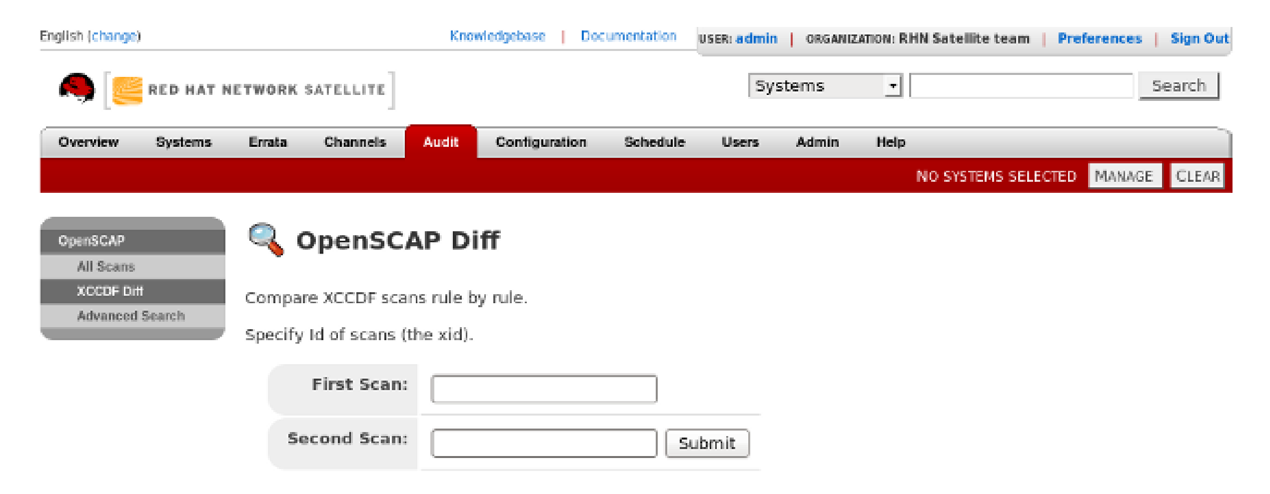


Abbildung 6.3. Prüfen ⇒ XCCDF Diff

Sie können auf das **diff** von ähnlichen Scans direkt zugreifen, indem Sie auf das Icon auf der Seite **Scans auflisten** klicken, oder Sie können ein **diff** von beliebigen Scans erstellen, indem Sie deren IDs angeben.

Objekte, die nur in einem der verglichenen Scans auftreten, werden als "unterschiedliche" Elemente betrachtet. Unterschiedliche Objekte sind in beige hervorgehoben. Es gibt drei Vergleichsmodi: **Kompletter Abgleich**, bei dem alle Scanobjekte gezeigt werden, **Nur geänderte Objekte**, bei dem nur die geänderten Objekte angezeigt werden, sowie **Nur unveränderliche Objekte**, bei dem unveränderte oder ähnliche Objekte gezeigt werden.

Prüfen → Erweiterte Suche

Die Suchseite ermöglicht Ihnen das Durchsuchen Ihrer Scans anhand bestimmter Kriterien, so z.B.:

- Regelergebnisse
- Zielrechner
- Zeitspanne des Scans

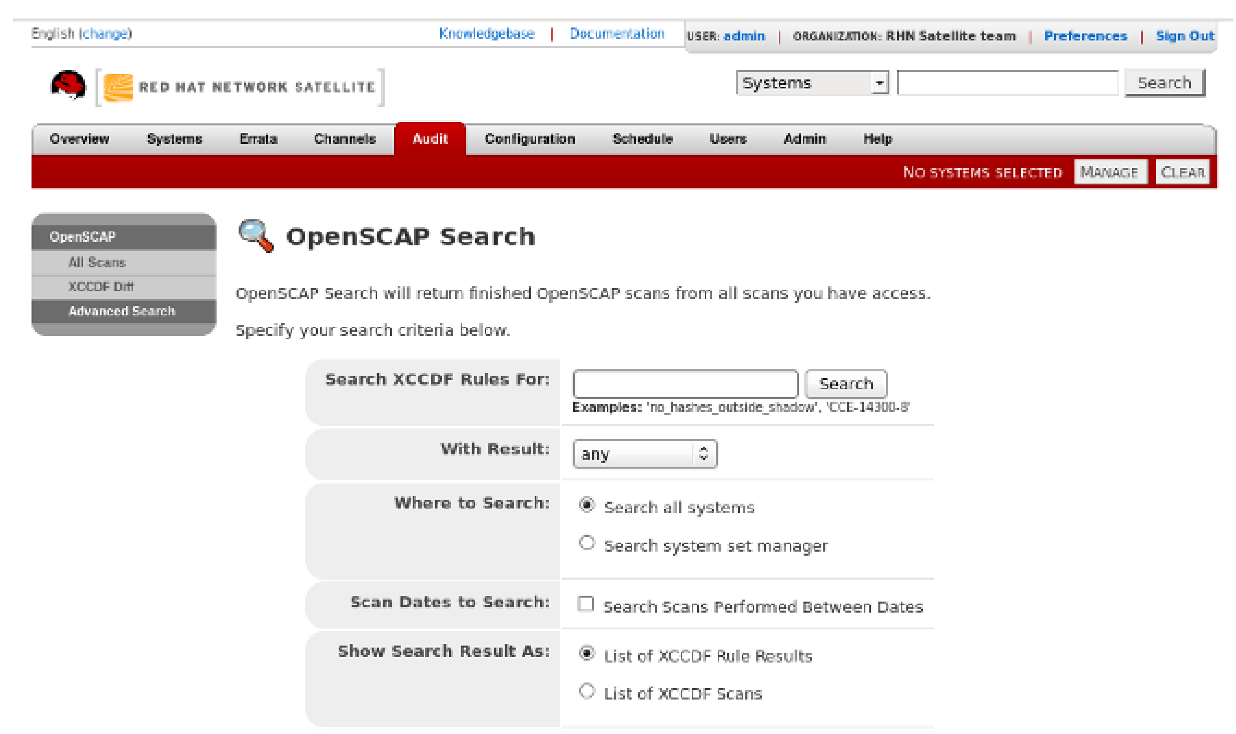


Abbildung 6.4. Prüfen ⇒ Erweiterte Suche

Die Suche gibt entweder eine Liste mit Ergebnissen aus oder eine Liste mit Scans, die in den Ergebnissen enthalten sind.

6.2.4.2. Systeme → Systemdetails → Prüfen

Dieser Reiter samt Unterreitern ermöglicht Ihnen das Einplanen und Anzeigen von Konformitätsscans für das System. Ein Scan wird vom SCAP-Tool durchgeführt, das den NIST-Standard SCAP (Security Content Automation Protocol) implementiert. Um das System zu scannen, vergewissern Sie sich, dass der SCAP-Inhalt vorbereitet ist und die Voraussetzungen in Abschnitt 6.2.1, „Voraussetzungen“ erfüllt sind.

Systeme → Systemdetails → Prüfen → Scans auflisten

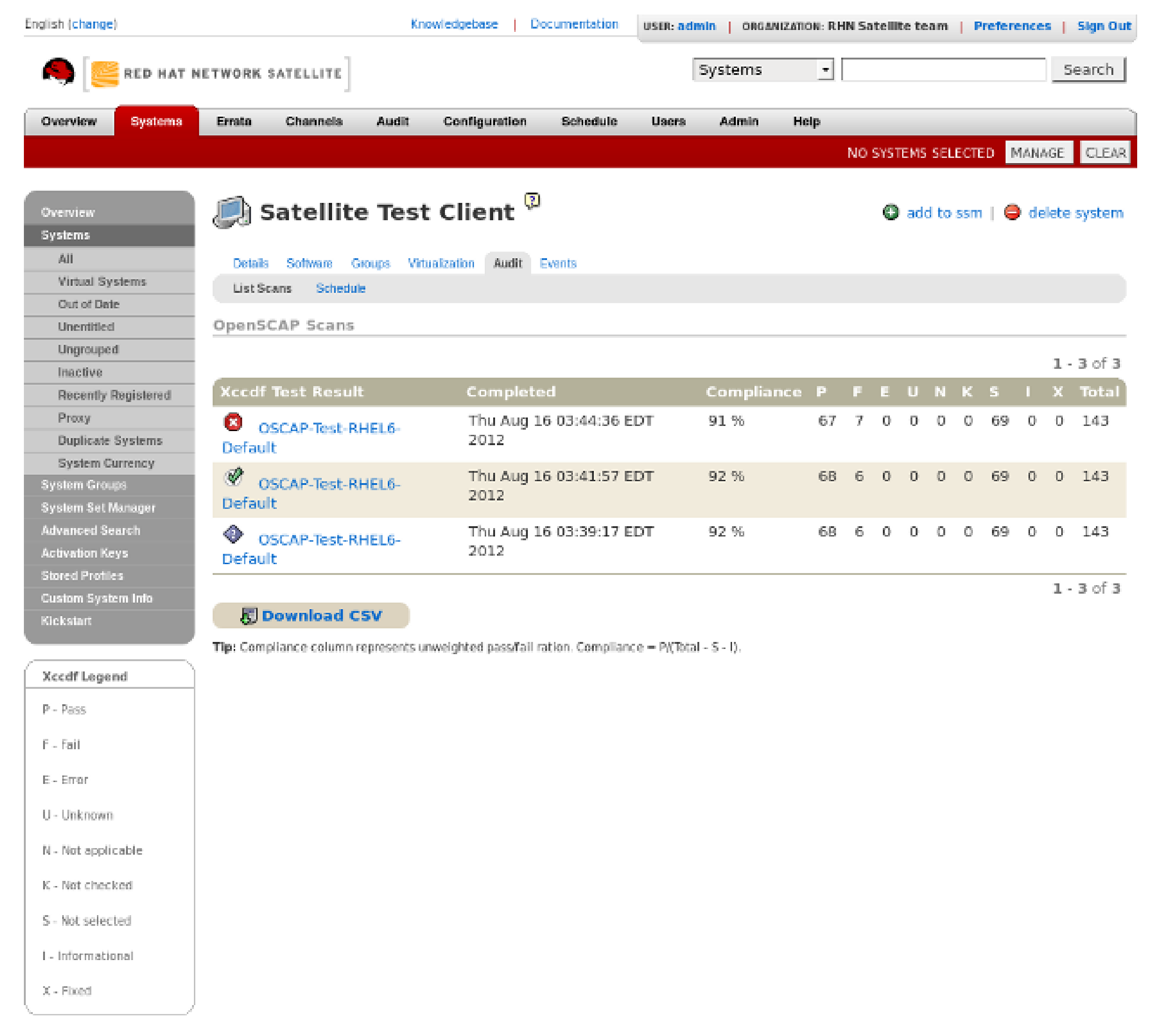


Abbildung 6.5. Systeme ⇒ Systemdetails ⇒ Prüfen ⇒ Scans auflisten, Scan-Ergebnisse

Dieser Unterreiter zeigt eine Zusammenfassung aller abgeschlossenen Scans auf dem System. Folgende Spalten werden angezeigt:

Tabelle 6.1. OpenSCAP Scan-Labels

Spalten-Label	Definition
XCCDF-Testergebnis	Der Testergebnis-Name des Scans mit Link zu detaillierten Ergebnissen
Abgeschlossen	Die genaue Zeit, an der der Scan abgeschlossen wurde
Konformität	Ungewichtetes erfolgreich/fehlgeschlagen-Verhältnis der Konformität mit dem verwendeten Standard
P	Anzahl der Prüfungen, die erfolgreich waren
F	Anzahl der Prüfungen, die fehlgeschlagen sind
E	Aufgetretene Fehler im Scan
U	Unbekannt
N	Nicht auf die Maschine zutreffend
K	Nicht geprüft
S	Nicht ausgewählt
I	Informationell
X	Behoben
Gesamt	Gesamtanzahl der Prüfungen

Jede Zeile beginnt mit einem Icon, das das Ergebnis eines Vergleichs zu einem vorherigen ähnlichen Scan anzeigt. Das Icon zeigt an, dass der neuere Scan entweder:

- — keinen Unterschied zum vorherigen Scan aufweist
- — einige Unterschiede aufweist
- — wesentliche Unterschiede aufweist, entweder sind mehr Prüfungen fehlgeschlagen oder weniger erfolgreich verlaufen als im vorherigen Scan
- — kein vergleichbarer Scan wurde gefunden, somit wurde kein Vergleich angestellt.

Systeme → Systemdetails → Prüfen → Scan-Details

Diese Seite enthält die Ergebnisse eines einzelnen Scans. Sie kann in zwei Teile unterteilt werden:

- Details des XCCDF-Scans

  Die Details des Scans umfassen:

  - die allgemeinen Informationen des Dateipfads
  - welche Befehlszeilenparameter verwendet wurden
  - wer ihn eingeplant hat
  - die Benchmark-Kennzeichnung und -Version
  - die Profilkennzeichnung
  - den Profiltitel
  - wann er gestartet und abgeschlossen wurde

- sowie etwaige Fehlerausgabe.

- XCCDF-Regelergebnisse

  Das Regelergebnis zeigt die vollständige Liste mit XCCDF-Regelkennzeichnungen, Tags und das Ergebnis für jede dieser Regelergebnisse. Diese Liste kann nach einem bestimmten Ergebnis gefiltert werden.

Systeme → Systemdetails → Prüfen → Plan

Auf diesem Unterreiter können neue Scans eingeplant werden. Zusätzliche Befehlszeilenparameter können angegeben werden, sowie der Pfad zum XCCDF-Dokument auf dem System, das gescannt wird. Basierend auf dem "**`Nicht früher einplanen als`**" Parameter wird der Scan bei der nächsten Anmeldung des Systems beim Satellite-Server gescannt. Weitere Informationen über das Einplanen über die Satellite-Weboberfläche finden Sie in Prozedur 6.1, „Scans über die Weboberfläche“ in diesem Kapitel.

Kapitel 7. PAM-Authentifizierung

RHN Satellite Server unterstützt netzwerkbasierte Authentifizierungssysteme mittels der sog. "Pluggable Authentication Modules" (PAM). PAM enthält eine Reihe von Bibliotheken, die Systemadministratoren dabei helfen, den RHN Satellite Server in ein zentralisiertes Authentifizierungsverfahren einzubinden, wodurch weniger Passwörter erinnert werden müssen.

RHN Satellite Server ist dazu in der Lage, PAM mit LDAP, Kerberos, Directory Server und anderen netzwerkbasierten Authentifizierungssystemen zu nutzen. Dieses Kapitel beschreibt, wie Sie PAM zum Einsatz in der Authentifizierungsinfrastruktur Ihres Unternehmens einrichten.

Prozedur 7.1. Einrichten der PAM-Authentifizierung

1. Vergewissern Sie sich, dass Sie die neueste Version des **selinux-policy-targeted**-Pakets haben:

   ```
   # yum update selinux-policy-targeted
   ```

2. Setzen Sie die SELinux boolesche Variable **allow_httpd_mod_auth_pam** auf:

   ```
   # setsebool -P allow_httpd_mod_auth_pam 1
   ```

3. Öffnen Sie die **/etc/rhn/rhn.conf**-Datei in einem Texteditor Ihrer Wahl und fügen Sie die folgende Zeile hinzu. Dadurch wird eine PAM-Dienstdatei unter **/etc/pam.d/rhn-satellite** erstellt:

   ```
   pam_auth_service = rhn-satellite
   ```

4. Um die Authentifizierung einzurichten, öffnen Sie die **/etc/pam.d/rhn-satellite**-Dienstdatei in einem Texteditor Ihrer Wahl und fügen Sie die gewünschten Regeln hinzu. Weitere Informationen über die Konfiguration von PAM finden Sie im Kapitel *Pluggable Authentication Modules (PAM)* im *Red Hat Enterprise Linux Bereitstellungshandbuch*.



Anmerkung

Überprüfen Sie, ob die PAM-Authentifizierung korrekt funktioniert, bevor Sie sie für dem RHN Satellite Server verwenden.

Beispiel 7.1. Verwenden von PAM mit Kerberos auf einem Red Hat Enterprise Linux 5 i386 System

Dieses Beispiel aktiviert PAM mit Kerberos-Authentifizierung auf einem Red Hat Enterprise Linux 5 i386 System.

Öffnen Sie die **/etc/pam.d/rhn-satellite**-Dienstdatei in einem Texteditor Ihrer Wahl und fügen Sie die folgenden Regeln hinzu:

```
#%PAM-1.0
auth        required      pam_env.so
auth        sufficient    pam_krb5.so no_user_check
auth        required      pam_deny.so
account     required      pam_krb5.so no_user_check
```

Ändern Sie für Benutzer, die sich mittels Kerberos authentifizieren, das Passwort mit **kpasswd**. Ändern Sie das Passwort nicht auf der RHN Website, da auf diese Weise nur das lokale Passwort auf dem Satellite-Server geändert würde. Lokale Passwörter werden nicht verwendet, wenn PAM für diesen Benutzer aktiviert ist.

Beispiel 7.2. Verwenden von PAM mit LDAP

Dieses Beispiel aktiviert PAM mit LDAP-Authentifizierung.

Öffnen Sie die **/etc/pam.d/rhn-satellite**-Dienstdatei in einem Texteditor Ihrer Wahl und fügen Sie die folgenden Regeln hinzu:

```
#%PAM-1.0
auth        required      pam_env.so
auth        sufficient    pam_ldap.so no_user_check
auth        required      pam_deny.so
account     required      pam_ldap.so no_user_check
```

Kapitel 8. RPMs

Als Teil von automatisierten Installationen implementieren Administratoren oft angepasste Applikationen, die nicht von Red Hat stammen, wie z.B. Backup- und Überwachungssoftware. Dazu muss diese Software als RPMs paketiert vorliegen. Eine Umgebung zum Erstellen von RPMs kann auf einem System eingerichtet werden, auf dem Red Hat Enterprise Linux läuft. Dazu ist anzumerken, dass das Build-System dieselbe Version von Paketen enthalten muss, die auch auf den Zielsystemen verwendet werden. Das bedeutet, dass ein Red Hat Enterprise Linux 5 System verwendet werden muss, um RPMs für Red Hat Enterprise Linux 5 Systeme zu erzeugen und ein Red Hat Enterprise Linux 6 System für Red Hat Enterprise Linux 6 RPMs.

Mindestens das **`rpm-build`**-Paket muss auf dem Build-System installiert sein. Unter Umständen benötigen Sie darüber hinaus weitere Pakete wie z.B. Compiler und Bibliotheken.

Produktionsbereite RPM-Pakete sollten mit einem GPG-Schlüssel signiert werden, anhand dessen die Quelle und die Integrität von Paketen überprüft werden kann. Die Passphrase des GPG-Schlüssels zur Signierung von RPMs sollte nur einer vertrauenswürdigen Gruppe von Administratoren bekannt sein.

Prozedur 8.1. Erstellen eines GPG-Schlüssels



Wichtig

Die folgenden Befehle initiieren die Erstellung eines GPG-Schlüssels und exportieren diesen in einem Format, das zur Verteilung an die Client-Systeme geeignet ist. Der erstellte Schlüssel sollte sicher verwahrt werden und eine Sicherungskopie angelegt werden.

1. Erstellen Sie ein Verzeichnis zum Erstellen des Schlüssels:

```
mkdir -p ~/.gnupg
```

2. Generieren Sie das Schlüsselpaar:

```
gpg --gen-key
```

Sie müssen die Art der Schlüssel, deren Größe und deren Gültigkeitsdauer festlegen (drücken Sie die **`Eingabe`**-Taste, um die Standardwerte zu übernehmen). Sie müssen zudem einen Namen, einen Kommentar und eine E-Mail-Adresse angeben:

```
Real name: rpmbuild
Email address: rpmbuild@example.com
Comment: this is a comment
You selected this USER-ID:
    "rpmbuild (this is a comment) <rpmbuild@example.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
```

Drücken Sie **`O`**, um die Details zu bestätigen und fortzufahren.

3. Listen Sie alle Schlüssel samt Fingerabdrücke auf:

```
gpg --list-keys --fingerprint
```

4. Exportieren Sie die Schlüssel:

```
gpg --export --armor "rpmbuild <rpmbuild@example.com>" > EXAMPLE-RPM-GPG-
KEY
```

5. Importieren Sie den Schlüssel in die RPM-Datenbank, so dass die Quelle und Integrität der RPMs durch Ausführen von **gpg --import** als Root auf allen Zielsystemen überprüft werden kann:

```
rpm --import EXAMPLE-RPM-GPG-KEY
```

   Dies erfolgt während der Client-Installationen automatisch und sollte nicht manuell ausgeführt werden müssen.

6. Sobald ein RPM erstellt wurde, kann es mit dem GPG-Schlüssel signiert werden und zum richtigen Channel hochgeladen werden:

```
rpm --resign package.rpm
rhnpush --server=http[s]://satellite.server/APP package.rpm --
channel=custom-channel-name
```

7. Um ein RPM-Paket zu überprüfen, navigieren Sie zum Verzeichnis, welches das fragliche Paket enthält, und führen Sie die folgenden Befehle aus:

```
rpm –qip package.rpm
rpm -K package.rpm
```

Prozedur 8.2. Erstellen von RPMs

1. Erstellen Sie ein nicht-privilegiertes Benutzerkonto namens **rpmbuild** zum Erzeugen von Paketen. Dadurch können mehrere Administratoren die Build-Umgebung und den GPG-Schlüssel gemeinsam nutzen.
2. Erstellen Sie im Benutzerverzeichnis des **rpmbuild**-Benutzers (**/home/rpmbuild**) eine Datei namens **.rpmmacros**:

```
touch /home/rpmbuild/.rpmmacros
```

3. Öffnen Sie die **.rpmmacros**-Datei in einem Texteditor Ihrer Wahl und fügen Sie die folgenden Zeilen hinzu. Der ***_gpg_name*** muss mit dem Namen des GPG-Schlüssels übereinstimmen, der zum Signieren der RPMs verwendet wird:

```
%_topdir             %(echo $HOME)/rpmbuild
%_signature         %gpg
%_gpg_name           rpmbuild <rpmbuild@example.com>
```

   Das Verzeichnis-Listing für das angegebene Verzeichnis oberster Ebene (im obigen Beispiel **/home/rpmbuild/rpmbuild**) muss dieselbe Verzeichnisstruktur aufweisen wie die unter **/usr/src/redhat**.

Beispiel 8.1. RPM-Spezifikationsdatei

Sehen Sie im Folgenden ein einfaches Beispiel einer RPM-Spezifikationsdatei. Beim Erstellen von RPMs sollte diese sich im **SPECS**-Verzeichnis unter dem **_topdir** befinden, wie in der **.rpmmacros**-Datei des Benutzers definiert. Die entsprechenden Quell- und Patch-Dateien sollten sich im **SOURCES**-Verzeichnis befinden.

```
Name: foo
Summary: The foo package does foo
Version: 1.0
Release: 1
License: GPL
Group: Applications/Internet
URL: http://www.example.org/
Source0 : foo-1.0.tar.gz
Buildroot: %{_tmppath}/%{name}-%{version}-%{release}-root
Requires: pam
BuildPrereq: coreutils
%description
This package performs the foo operation.
%prep
%setup -q
%build
%install
mkdir -p %{buildroot}/%{_datadir}/%{name}
cp -p foo.spec %{buildroot}/%{_datadir}/%{name}
%clean
rm -fr %{buildroot}
%pre
# Add user/group here if needed
%post
/sbin/chkconfig --add food
%preun
if [ $1 = 0 ]; then # package is being erased, not upgraded
    /sbin/service food stop > /dev/null 2>&1
    /sbin/chkconfig --del food
fi
%postun
if [ $1 = 0 ]; then # package is being erased
    # Any needed actions here on uninstalls
else
    # Upgrade
    /sbin/service food condrestart > /dev/null 2>&1
fi
%files
%defattr(-,root,root)
%{_datadir}/%{name}
%changelog
* Mon Jun 16 2003 Some One <one@example.com>
- fixed the broken frobber (#86434)
```

Kapitel 9. Boot-Geräte

Die automatisierte Installation (oder *Kickstart*) ist ein wesentlicher Aspekt beim effizienten Provisioning von Systemen. Dieses Kapitel beschreibt, wie verschiedene Arten von Boot-Medien zum Kickstarten von Clients vorbereitet werden.

Detailliertere Informationen über den Einsatz von Kickstarts beim Provisioning finden Sie im *RHN Satellite Server Handbuch zum Einstieg*.

Das Red Hat Enterprise Linux CD Boot-Image **`boot.iso`** ist eine erforderliche Voraussetzung zum Erstellen von Boot-Geräten. Stellen Sie sicher, dass es auf dem System verfügbar ist und notieren Sie sich dessen Speicherort.

Prozedur 9.1. CD Boot-Medium



Anmerkung

Das Backslash-Zeichen "\" wird nachfolgend verwendet um anzuzeigen, dass diese Zeile am Shell-Prompt in derselben Zeile fortgeführt werden soll.

1. Erstellen Sie ein Arbeitsverzeichnis für das Boot-Image:

```
mkdir -p temp cd/isolinux
```

2. Hängen Sie das Boot-Image im **`temp`**-Verzeichnis ein:

```
mount -o loop boot.iso temp
```

3. Kopieren Sie die erforderlichen Dateien für ein CD-Medium-Bootgerät in das zuvor erstellte Verzeichnis:

```
cp -aP temp/isolinux/* cd/isolinux/
```

4. Hängen Sie das **`temp`**-Verzeichnis aus und ändern Sie die Berechtigungen auf dem **`cd`**-Verzeichnis, um es für den Benutzer les- und schreibbar zu machen:

```
umount temp
chmod -R u+rw cd
```

5. Wechseln Sie in das **`./cd`**-Verzeichnis:

```
cd ./cd
```

6. Kopieren Sie die **`/usr/lib/syslinux/menu.c32`**-Datei auf die CD:

```
cp -p /usr/lib/syslinux/menu.c32 isolinux
```

7. Öffnen Sie die **`isolinux/isolinux.cfg`**-Datei in einem Texteditor Ihrer Wahl und fügen Sie die folgende Zeile hinzu:

```
mkisofs -o ./custom-boot.iso -b isolinux/isolinux.bin -c isolinux/boot.cat -
no-emul-boot \
  -boot-load-size 4 -boot-info-table -J -l -r -T -v -V "Custom RHEL Boot" .
```

8. Passen Sie die Boot-Parameter und Ziele in **isolinux.cfg** für das Booten von CD an.
9. Brennen Sie die Daten auf die CD, um den Vorgang abzuschließen.

Prozedur 9.2. PXE Boot

1. Erstellen Sie ein Arbeitsverzeichnis für das Boot-Image:

```
mkdir -p temp pxe/pxelinux.cfg
```

2. Hängen Sie das Boot-Image im **temp**-Verzeichnis ein:

```
mount -o loop boot.iso temp
```

3. Kopieren Sie die erforderlichen Dateien für ein PXE-Bootgerät in das zuvor erstellte Verzeichnis:

```
cp -aP temp/isolinux/* pxe/
```

4. Hängen Sie das **temp**-Verzeichnis aus und ändern Sie die Berechtigungen auf dem **cd**-Verzeichnis, um es für den Benutzer les- und schreibbar zu machen:

```
umount temp
chmod -R u+rw pxe
```

5. Wechseln Sie in das **/pxe**-Verzeichnis:

```
cd ./pxe
```

6. Kopieren Sie die **/usr/lib/syslinux/menu.c32**-Datei in das **/pxe**-Verzeichnis:

```
cp -p /usr/lib/syslinux/menu.c32 .
```

7. Verschieben Sie die **isolinux.cfg**-Datei nach **pxelinux.cfg/default**:

```
mv isolinux.cfg pxelinux.cfg/default
```

8. Löschen Sie die temporären Dateien:

```
rm -f isolinux.bin TRANS.TBL
```

9. Kopieren Sie die **/usr/lib/syslinux/pxelinux.0**-Datei in das **/pxe**-Verzeichnis:

```
cp -p /usr/lib/syslinux/pxelinux.0 .
```

10. Öffnen Sie die **pxelinux.cfg/default**-Datei in einem Texteditor Ihrer Wahl und passen Sie die Boot-Parameter und Ziele für das PXE Booten an.

Prozedur 9.3. USB Boot-Medium



Warnung

Seien Sie extrem vorsichtig, wenn Sie diese Befehle als Root ausführen (für die meisten der kritischen Stellen ist dies erforderlich). Diese Befehle greifen auf die Gerätedateien zu, und eine fehlerhafte Änderung könnte Ihr System unter Umständen irreparabel beschädigen. Das nachfolgende Beispiel nutzt **`/dev/loop0`** zum Einhängen; stellen Sie sicher, dass Sie das korrekte Gerät für Ihr System verwenden. Mit dem Befehl **`losetup -f`** können Sie überprüfen, welches Gerät das richtige ist.

1. Erstellen Sie ein Arbeitsverzeichnis für das Boot-Image:

   ```
   mkdir -p temp usb/extlinux
   ```

2. Hängen Sie das Boot-Image im **`temp`**-Verzeichnis ein:

   ```
   mount -o loop boot.iso temp
   ```

3. Kopieren Sie die erforderlichen Dateien für ein USB-Medium-Bootgerät in das zuvor erstellte Verzeichnis:

   ```
   cp -aP temp/isolinux/* usb/extlinux/
   ```

4. Hängen Sie das **`temp`**-Verzeichnis aus und ändern Sie die Berechtigungen auf dem **`cd`**-Verzeichnis, um es für den Benutzer les- und schreibbar zu machen:

   ```
   umount temp
   chmod -R u+rw usb
   ```

5. Wechseln Sie in das **`/usb`**-Verzeichnis:

   ```
   cd ./usb
   ```

6. Kopieren Sie die **`/usr/lib/syslinux/menu.c32`**-Datei in das **`extlinux/`**-Verzeichnis:

   ```
   cp -p /usr/lib/syslinux/menu.c32 extlinux/
   ```

7. Verschieben Sie die **`extlinux/isolinux.cfg`**-Datei nach **`extlinux/extlinux.conf`**:

   ```
   mv extlinux/isolinux.cfg extlinux/extlinux.conf
   ```

8. Löschen Sie die temporären Dateien:

   ```
   rm -f extlinux/isolinux.bin extlinux/TRANS.TBL
   ```

9. Konvertieren Sie die **`custom-boot.img`**-Datei und kopieren Sie sie:

   ```
   dd if=/dev/zero of=./custom-boot.img bs=1024 count=30000
   ```

10. Bestimmen Sie den richtigen Einhängepunkt für das Loopback-Gerät:

```
losetup -f
/dev/loop0
```

Richten Sie das Loopback-Gerät mit dem Boot-Image ein:

```
losetup /dev/loop0 ./custom-boot.img
```

11. Öffnen Sie das **fdisk**-Dienstprogramm:

```
fdisk /dev/loop0
```

Erstellen Sie eine primäre, bootbare Partition auf dem Gerät. Sie erreichen dies durch Drücken der folgenden Tasten: **n p 1 Eingabe Eingabe a 1 p w**

12. Kopieren Sie den Master Boot Record (MBR) auf das Loopback-Gerät:

```
dd if=/usr/lib/syslinux/mbr.bin of=/dev/loop0
```

13. Fügen Sie Partitionszuordnungen zum Loopback-Gerät hinzu:

```
kpartx -av /dev/loop0
```

14. Erzeugen Sie das Dateisystem:

```
mkfs.ext2 -m 0 -L "Custom RHEL Boot" /dev/mapper/loop0p1
```

15. Hängen Sie das Gerät ein:

```
mount /dev/mapper/loop0p1 temp
```

16. Löschen Sie temporäre Dateien:

```
rm -rf temp/lost+found
```

17. Kopieren Sie das **extlinux/**-Verzeichnis an einen temporären Speicherort:

```
cp -a extlinux/* temp/
```

18. Installieren Sie den Bootloader an diesem temporären Speicherort:

```
extlinux temp
```

19. Hängen Sie den temporären Speicherort aus:

```
umount temp
```

20. Löschen Sie die Partitionszuordnungen auf dem Loopback-Gerät:

```
kpartx -dv /dev/loop0
```

21. Löschen Sie das Loopback-Gerät:

```
losetup -d /dev/loop0
```

Synchronisieren Sie die Änderungen am Dateisystem:

```
sync
```

22. Öffnen Sie die **`extlinux.conf`**-Datei in einem Texteditor Ihrer Wahl und passen Sie die Boot-Parameter und Ziele für das Booten von USB an.
23. Übertragen Sie das Image auf ein USB-Gerät, um das Verfahren abzuschließen. Stecken Sie das USB-Gerät ein und führen den **`dmesg`**-Befehl aus, um den Einhängepunkt zu überprüfen. In diesem Beispiel ist dies **`/dev/sdb`**.

    Hängen Sie das USB-Gerät aus:

    ```
    umount /dev/sdb
    ```

    Kopieren Sie das Image auf das USB-Gerät:

    ```
    dd if=./custom-boot.img of=/dev/sdb
    ```

Kapitel 10. Organisationen

RHN Satellite ermöglicht es Administratoren, Ihre Deployments in organisierte Container zu unterteilen. Diese Container (oder *Organisationen*) ermöglichen eine eindeutige Trennung von Zweck, Besitzer und Inhalten dieser Systeme.

RHN Satellite unterstützt die Erstellung und Verwaltung von multiplen *Organisationen* innerhalb einer Installation und ermöglicht so die Unterteilung von Systemen, Inhalten und Subskriptionen über verschiedene Gruppen hinweg. Dieses Kapitel fasst die wesentlichen Konzepte und Aufgaben zur Einrichtung und Verwaltung von multiplen Organisationen zusammen.

Auf der **`Organisationen`**-Weboberfläche können Administratoren multiple Satellite-Organisationen ansehen, erstellen und verwalten. Satellite-Administratoren können Software- und Systemberechtigungen über verschiedene Organisationen hinweg zuweisen und den Zugriff einer Organisation auf Aufgaben zur Systemverwaltung steuern.

Satellite-Administratoren können neue Organisationen erstellen und diesen Organisationen Administratoren und Berechtigungen zuweisen. Organisationsadministratoren können Gruppen, Systeme und Benutzer für ihre Organisation zuweisen. Diese Unterteilung erlaubt es Organisationen, administrative Aufgaben ohne Auswirkungen auf die anderen Organisationen selbst durchzuführen.

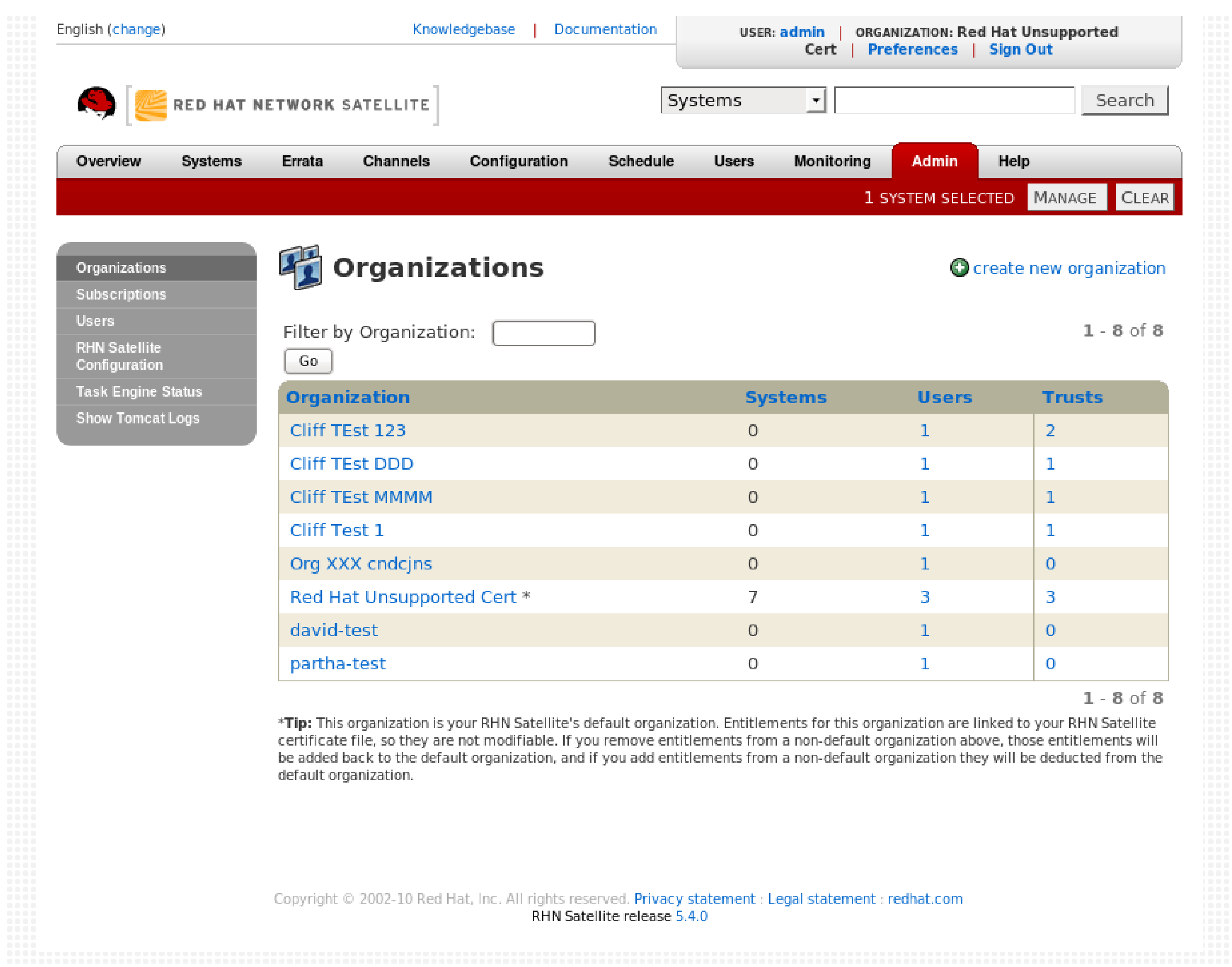


Abbildung 10.1. Admin

Die **`Organisationen`**-Seite enthält eine Aufstellung aller Organisationen auf dem Satellite, samt

Benutzer- und Systemanzahl für jede Organisation. Die **Organisationen**-Seite verfügt zudem über eine **Trusts**-Seite für eventuell eingerichtete Organisations-Trusts.

10.1. Erstellen von Organisationen

Prozedur 10.1. Erstellen einer Organisation

1. Um eine neue Organisation zu erstellen, öffnen Sie das **Admin**-Menü und wählen **Organisationen** => **Neue Organisation erstellen**.

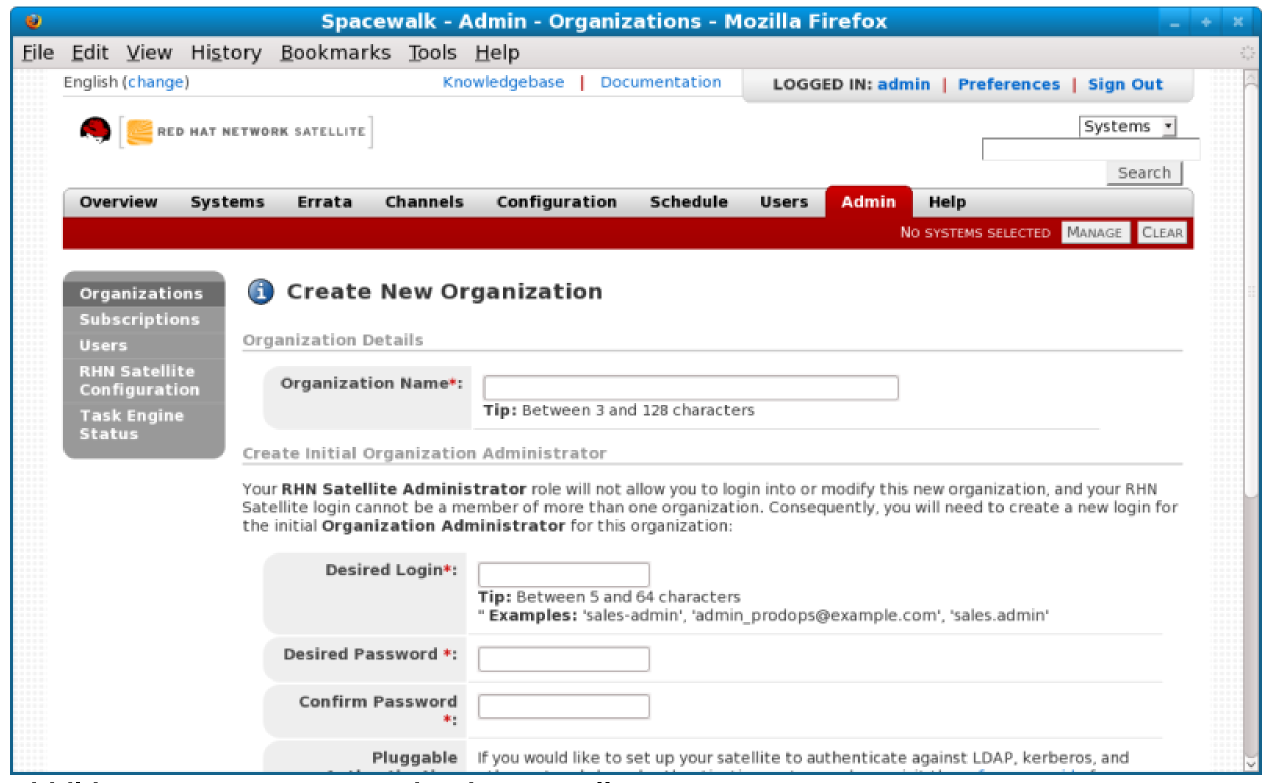


Abbildung 10.2. Neue Organisation erstellen

2. Geben Sie den Organisationsnamen im entsprechenden Textfeld ein. Der Name sollte zwischen 3 und 128 Zeichen lang sein.
3. Erstellen Sie einen Administrator für die Organisation, indem Sie die folgenden Informationen angeben:
   - Geben Sie ein **Gewünschtes Login** für den Organisationsadministrator an, welches zwischen 3 und 128 Zeichen lang sein sollte. Ziehen Sie einen aussagekräftigen Login-Namen für den Organisationsadministrator-Account in Erwägung, der den administrativen Login-Namen der Organisation entspricht.
   - Geben Sie ein **Gewünschtes Passwort** an und **Bestätigen** Sie es.
   - Geben Sie die **E-Mail**-Adresse des Organisationsadministrators an.
   - Geben Sie den **Vornamen** und **Nachnamen** des Organisationsadministrators ein.
4. Klicken Sie auf die Schaltfläche **Organisation erstellen**, um den Vorgang abzuschließen.

Sobald die neue Organisation erstellt wurde, wird die **Organisationen**-Seite mit der neu erstellten Organisation angezeigt.

Satellite-Administratoren sollten in Erwägung ziehen, den Organisationsadministrator-Account der ***Organisation 1*** sich selbst vorzubehalten, um die Möglichkeit zu haben, sich falls nötig bei dieser

Organisation anzumelden.



Wichtig

Wenn Ihr RHN Satellite für PAM-Authentifizierung konfiguriert ist, vermeiden Sie die Verwendung von PAM-Accounts für den Satellite administrativen Organisationsadministrator-Account in neuen Organisationen. Erstellen Sie stattdessen einen Account lokal auf dem Satellite für Organisationsadministratoren und reservieren die PAM-authentifizierten Accounts für Satellite-Logins mit niedrigeren Berechtigungen. So halten Sie Benutzer davon ab, sich häufig mit höheren Berechtigungen beim RHN Satellite anzumelden, da das Fehlerpotenzial mit diesen Accounts höher ist.

10.2. Verwalten der Berechtigungen

Nachdem Sie eine neue Organisation erstellt haben, ist es wichtig, ihr Berechtigungen zuzuweisen. Sie benötigen für jedes System Systemberechtigungen, wie z.B. Management und Provisioning. Sie benötigen außerdem Channel-Berechtigungen, wie z.B. **`rhel-server`** oder **`rhn-tools`**, für solche Systeme, die neben den angepassten Channels noch weitere Channels nutzen. Management-Systemberechtigungen sind eine Grundvoraussetzung, damit eine Organisation ordnungsgemäß funktionieren kann. Die Anzahl der Management-Berechtigungen, die einer Organisation zugewiesen werden, entspricht der Höchstanzahl an Systemen, die sich bei dieser Organisation auf dem RHN Satellite anmelden dürfen, ungeachtet der Anzahl der verfügbaren Software-Berechtigungen. Gibt es z.B. insgesamt 100 Red Hat Enterprise Linux Client-Berechtigungen, aber es stehen der Organisation nur 50 Management-Systemberechtigungen zur Verfügung, so können sich nur 50 Systeme bei dieser Organisation registrieren.

Es müssen außerdem Red Hat Network Tools Software-Channel-Berechtigungen an jede Organisation vergeben werden. Der Red Hat Network Tools Channel enthält verschiedene Client-Software, die für erweiterte RHN Satellite Funktionalität notwendig ist, wie z.B. nötige Clients zum Konfigurationsmanagement und zur Kickstart-Unterstützung sowie das **`rhn-virtualization`**-Paket, das notwendig ist, um die Berechtigungen von Xen und KVM virtualisierten Gästen korrekt zu zählen.

Um auf die **`Subskriptionen`**-Oberfläche zu gelangen, öffnen Sie das **Admin**-Menü und wählen **`Organisationen`**. Wählen Sie eine Organisation aus der Liste und klicken Sie auf den **`Subskriptionen`**-Reiter.

Öffnen Sie auf der **`Subskriptionen`**-Oberfläche den Reiter **`Software-Channel-Berechtigungen`**, um alle Berechtigungen für alle Organisationen samt deren Verbrauch anzuzeigen.

Auf dem **`Software-Channel-Berechtigungen`**-Reiter können Satellite-Administratoren auf dem **`Organisationen`**-Reiter die Anzahl der Software-Channels anpassen, die jeder Organisation zur Verfügung stehen. Geben Sie die Anzahl ein (innerhalb des in **`Mögliche Werte`** genannten Bereichs) und klicken anschließend die Schaltfläche **`Aktualisieren`**, um diesen Wert zu ändern.

Channel-Berechtigungen sind entweder *Regulär* oder *Flex*. Jedes System kann eine reguläre Berechtigung verbrauchen. Flex-Berechtigungen dagegen können nur von Systemen genutzt werden, die als Gäste eines unterstützten Virtualisierungstyps erkannt wurden.



Anmerkung

Organisationsadministratoren, die einen angepassten Channel erstellen, können diesen Channel nur innerhalb ihrer Organisation verwenden, es sei denn, es wurde ein Organisations-Trust zwischen den Organisationen eingerichtet, die den Channel gemeinsam verwenden möchten. Weitere Informationen über Organisations-Trusts finden Sie in Abschnitt 10.5, „Organisations-Trusts“.

Der **Organisationen**-Reiter enthält einen Abschnitt **Subskriptionen**+**System-Berechtigungen** mit folgenden Details:

- **Insgesamt**: Die Gesamtanzahl an Channel-Berechtigungen für den Satellite.
- **Verfügbar**: Die Anzahl an Berechtigungen, die derzeit zur Zuweisung verfügbar sind.
- **Verbrauch**: Die Anzahl an Berechtigungen, die derzeit von allen Organisationen in Gebrauch sind, im Vergleich zur Gesamtanzahl der zugewiesenen Berechtigungen.

Weist die **Insgesamt**-Spalte beispielsweise 100 aus und die **Verfügbar**-Spalte 70, bedeutet dies, dass 30 Berechtigungen Organisationen zugewiesen sind. Die **Verbrauch**-Spalte zeigt, wieviele dieser 30 zugewiesenen Berechtigungen von Organisationen außer der Basisorganisation in Gebrauch sind. Lautet die **Verbrauch**-Spalte **24 von 30 (80%)**, bedeutet dies, dass 24 Channel-Berechtigungen an Satellite-Organisationen vergeben sind (ausgenommen der ***Organisation 1***) von 30 insgesamt zugewiesenen.

Wählen Sie auf der **Subskriptionen**-Oberfläche den Reiter **Software-Channel-Berechtigungen**, um alle Berechtigungen über alle Organisationen hinweg samt deren Verbrauch einzusehen. Klicken Sie auf eine Organisation, um die **Details**-Seite anzuzeigen, die weitere Informationen über die Organisation liefert.

- **Aktive Benutzer**: Die Anzahl von Benutzern in der Organisation
- **Systeme**: Die Anzahl von Systemen, die bei dieser Organisation angemeldet sind.
- **Systemgruppen**: Die Anzahl von Gruppen, die bei dieser Organisation angemeldet sind.
- **Aktivierungsschlüssel**: Die Anzahl von Aktivierungsschlüsseln, die dieser Organisation zur Verfügung stehen.
- **Kickstart-Profile**: Die Anzahl von Kickstart-Profilen, die dieser Organisation zur Verfügung stehen.
- **Konfigurations-Channels**: Die Anzahl von Konfigurations-Channels, die dieser Organisation zur Verfügung stehen.

Auf dieser Seite können Sie die Organisation löschen, indem Sie auf den Link **Organisation löschen** klicken.

10.3. Konfigurieren von Systemen in einer Organisation

Sobald eine Organisation erstellt wurde und ihr Berechtigungen zugewiesen wurden, können der Organisation nun Systeme zugewiesen werden.

Es gibt zwei Arten, auf die Sie ein System bei einer bestimmten Organisation registrieren können:

Registrierung mittels Benutzername und Passwort

Wenn Sie einen Benutzernamen und ein Passwort angeben, die für eine bestimmte

Organisation erzeugt wurden, wird das System bei dieser Organisation registriert. Ist beispielsweise **user-123** ein Mitglied der **Central IT** Organisation auf dem Satellite, so würde der folgende Befehl - ausgeführt auf einem beliebigen System - dieses System bei der **Central IT** Organisation auf Ihrem Satellite registrieren:

```
rhnreg_ks --username=user-123 --password=foobar
```



Anmerkung

Die ***--orgid***-Parameter in **rhnreg_ks** hängen *nicht* mit der Satellite-Registrierung oder RHN Satellites Unterstützung für multiple Organisationen zusammen.

Registrierung mittels Aktivierungsschlüssel

Sie können ein System auch mithilfe eines Aktivierungsschlüssels der Organisation registrieren. Aktivierungsschlüssel registrieren Systeme bei derjenigen Organisation, in der dieser Aktivierungsschlüssel erzeugt wurde. Aktivierungsschlüssel sind eine gute Registrierungsmethode, wenn Sie Benutzern erlauben möchten, Systeme bei einer Organisation zu registrieren, ohne ihnen Zugriffsrechte auf diese Organisation zu gewähren.

```
rhnreg_ks --activationkey=21-myactivationkey
```

Wenn Sie Systeme zwischen Organisationen verschieben möchten, können Sie dies mithilfe von Skripten ebenfalls unter Verwendung der Aktivierungsschlüssel automatisieren.



Anmerkung

Die ersten Zeichen des Aktivierungsschlüssels zeigen an, welche Organisation (nach ID-Nummer) Besitzer dieses Schlüssels ist.

10.4. Benutzer einer Organisation

Die **Benutzer**-Seite enthält eine Liste aller Benutzer auf dem Satellite, über alle Organisationen hinweg.

Die **Benutzer**-Seite listet die Benutzer auf, die dieser Organisation zugewiesen sind, einschließlich ihrer realen Namen, E-Mail-Adressen und einem Auswahlkästchen, das anzeigt, ob dieser Benutzer ein Organisationsadministrator ist.

Falls Sie der Organisationsadministrator sind, können Sie den Benutzernamen anklicken, um die **Benutzerdetails**-Seite für diesen Benutzer anzuzeigen.



Anmerkung

Sie müssen als Organisationsadministrator angemeldet sein, um die Benutzerdetails für eine Organisation zu verändern. Die Satellite-Administrator-Rolle erlaubt Ihnen nicht das Ändern von Benutzerdetails für Organisationsbenutzer, sie erlaubt Ihnen lediglich, anderen Benutzern innerhalb des Satellites die Satellite-Administrator-Rolle zuzuweisen.

10.5. Organisations-Trusts

Organisationen können Ihre Ressourcen miteinander teilen, indem Sie eine Verbindung als Organisations-Trust (eine Vertrauensbeziehung) eingehen. Organisations-Trusts werden vom Satellite-Administrator definiert und können vom Organisationsadministrator implementiert werden. Sobald ein Satellite-Administrator einen Trust zwischen zwei oder mehr Organisationen erstellt hat, steht es den Organisationsadministratoren jeder dieser Organisationen frei, so viel oder so wenig Ihrer Ressourcen zu teilen, wie sie möchten. Es ist die Entscheidung eines jeden Organisationsadministrators, welche Ressourcen zur gemeinsamen Verwendung freigegeben werden sollen, und welche freigegebenen Ressourcen von anderen Organisationen im Trust genutzt werden.

Jede individuelle Beziehung ist eindeutig und bleibt unberührt von den anderen Vertrauensbeziehungen der anderen Organisation. Zum Beispiel: Wenn die Buchhaltungs-Organisation der Finanzen-Organisation vertraut, und die Finanzen-Organisation der Betriebsmittel-Organisation, dann wird die Buchhaltungs-Organisation nicht notwendigerweise der Betriebsmittel-Organisation vertrauen, es sei denn, es wird eine separate Vertrauensbeziehung zwischen ihnen eingerichtet.

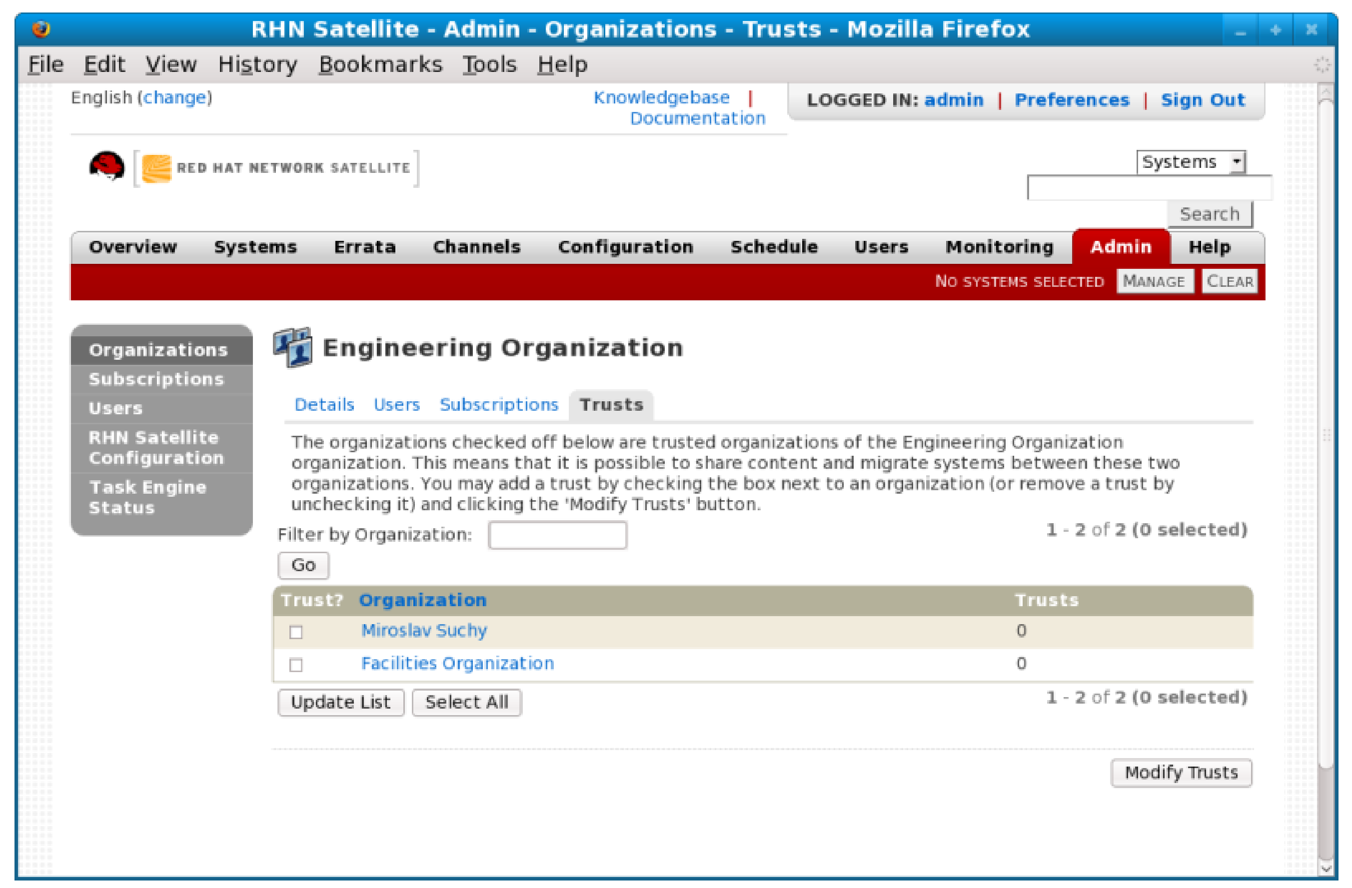


Abbildung 10.3. Organisations-Trusts

Prozedur 10.2. Einrichten eines Organisations-Trusts

Ein Satellite-Administrator kann einen Trust (eine Vertrauensbeziehung) zwischen zwei oder mehreren Organisationen einrichten. Führen Sie dazu die folgenden Schritte aus:

1. Wählen Sie den **`Organisationen`**-Link im Menü der **`Admin`**-Seite.
2. Klicken Sie auf den Namen einer der Organisationen und wählen anschließend auf der **`Details`**-Seite den **`Trusts`**-Reiter.
3. Auf dem **`Trusts`**-Reiter sehen Sie eine Aufstellung aller anderen Trusts auf dem RHN Satellite. Falls Sie eine lange Liste mit Organisationen haben, können Sie das Textfeld **`Filtern nach Organisation`** nutzen, um sie zu filtern.
4. Klicken Sie auf das Auswahlkästchen neben den Namen derjenigen Organisationen, die mit der aktuellen Organisation einen Organisations-Trust bilden sollen.
5. Klicken Sie die Schaltfläche **`Trusts bearbeiten`**, um den Trust zu erstellen.

Sobald ein Organisations-Trust eingerichtet wurde, können Organisationen angepasste Software-Channels für die anderen Organisationen im Trust freigeben. Es gibt drei Stufen der Channel-Freigabe, die auf jeden Channel angewendet werden können, um den Zugriff zu steuern:

Privat

Kennzeichnen Sie den Channel als privat, damit dieser von keiner anderen Organisation außer der besitzenden Organisation genutzt werden kann.

Geschützt

Erlauben Sie den Zugriff auf diesen Channel nur bestimmten, von Ihnen ausgewählten Organisationen im Trust.

Öffentlich

Erlauben Sie allen Organisationen innerhalb des Trusts den Zugriff auf diesen angepassten Channel.

Vertrauenswürdige Organisationen, denen Zugriff auf die angepassten Inhalte gewährt wird - entweder im geschützten oder öffentlichen Zugriffsmodus - können Ihren Client-Systemen erlauben, Pakete von diesem freigegebenen Channel zu installieren und zu aktualisieren. In den folgenden Situationen kann der Subskriptionszugriff darauf jedoch verloren gehen:

- Der Satellite-Administrator löscht die Vertrauensbeziehung
- Der Organisationsadministrator ändert die Channel-Freigabe auf privat
- Der Organisationsadministrator ändert die Channel-Freigabe auf geschützt und fügt die Organisation des subskribierenden Systems nicht zu der Liste für geschützten Zugriff hinzu
- Der Organisationsadministrator löscht den freigegebenen Channel direkt
- Der Organisationsadministrator löscht den übergeordneten Channel eines freigegebenen Sub-Channels



Anmerkung

Sämtliche Red Hat Software-Channels werden mithilfe von Berechtigungen verwaltet. Organisationsadministratoren können keine Red Hat Channels freigeben, da diese allen Organisationen zur Verfügung stehen, die Berechtigungen zu diesen Channels haben. Der Satellite-Administrator ist dafür verantwortlich, Red Hat Software-Channel-Berechtigungen an jede Organisation zu vergeben.

Prozedur 10.3. Migration von Systemen

Zusätzlich zur gemeinsamen Verwendung von Software-Channels können Organisationen in einem Trust mithilfe des **`migrate-system-profile`**-Dienstprogramms auch Systeme auf andere Organisationen im Trust migrieren. Dieses Dienstprogramm wird von der Befehlszeile aus aufgerufen und verwendet die Parameter ***`systemID`*** und ***`orgID`***, um die Systemmigration und deren Zielorganisation zu spezifizieren. Der Satellite-Administrator kann ein System von einer beliebigen Organisation auf eine andere Organisation im Trust migrieren. Dagegen können Organisationsadministratoren lediglich ein System von ihrer eigenen Organisation auf eine andere Organisation im Trust migrieren.

Für den **`migrate-system-profile`**-Befehl muss das **`spacewalk-utils`**-Paket installiert sein, was normalerweise standardmäßig auf dem RHN Satellite installiert ist. Wenn eine Organisation mithilfe des **`migrate-system-profile`**-Befehls ein System migriert, übernimmt das System keine der früheren Berechtigungen oder Channel-Subskriptionen von der Quellorganisation. Allerdings wird die Chronik des Systems bewahrt und kann vom neuen Organisationsadministrator eingesehen werden, um den Rest des Migrationsvorgangs zu vereinfachen, wie z.B. das Subskribieren eines Basis-Channels und das Zuweisen von Berechtigungen.

1. Führen Sie den Befehl nach folgendem Schema aus:

   ```
   migrate-system-profile --satellite SATELLITE HOSTNAME OR IP --
   systemId=SYSTEM ID --to-org-id=DESTINATION ORGANIZATION ID
   ```

   Angenommen, die Finanzabteilung (im RHN Satellite angelegt als Organisation mit der ***`OrgID 2`***) möchte einen Arbeitsplatzrechner (mit der ***`SystemID 10001020`***) von der Entwicklungsabteilung migrieren, doch der Finanz-Organisationsadministrator hat keinen Shell-Zugriff auf den RHN Satellite Server. Der RHN Satellite Hostname ist **`satserver.example.com`**. Der Finanz-Organisationsadministrator würde in diesem Fall Folgendes am Shell-Prompt eingeben:

   ```
   migrate-system-profile --satellite satserver.example.com --systemId=10001020
   --to-org-id=2
   ```

   Das Dienstprogramm fragt daraufhin nach einem Benutzernamen und Passwort.

2. Das System kann dann auf der RHN Satellite Weboberfläche auf der **`Systeme`**-Seite eingesehen werden. Der Migrationsvorgang wird abgeschlossen, indem dem Client ein Basis-Channel und Berechtigungen zugewiesen werden für andere bei dieser Organisation registrierte Systeme, verfügbar auf der **`Verlauf`**-Seite des Systems unter dem **`Ereignisse`**-Unterreiter des Systems.

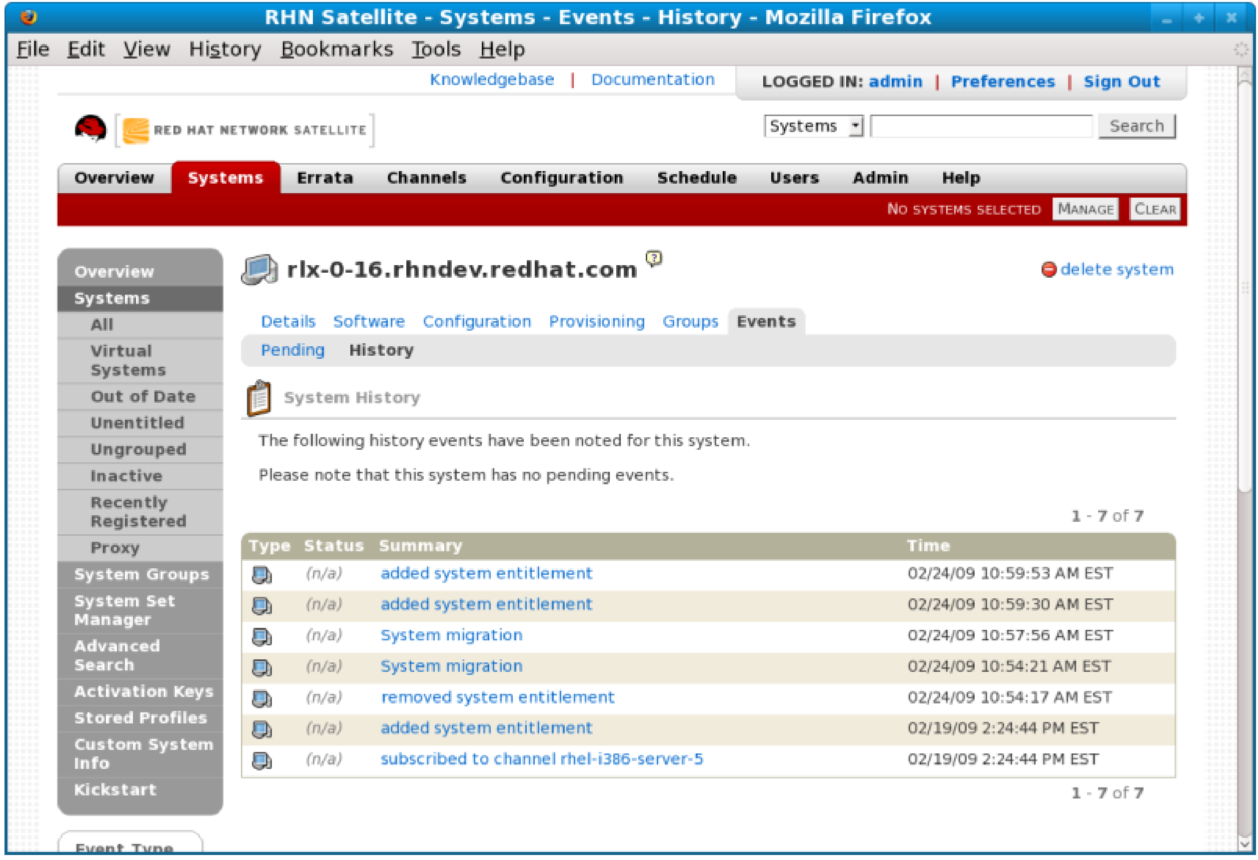


Abbildung 10.4. Systemverlauf

3. Satellite-Administratoren, die mehrere Systeme gleichzeitig migrieren müssen, können die Option **`--csv`** zum Befehl **`migrate-system-profile`** verwenden, um den Vorgang mithilfe einer einfachen kommagetrennten Liste der zu migrierenden System zu automatisieren.

   Eine Zeile in der CSV-Datei sollte die ID des zu migrierenden Systems enthalten sowie die ID der Zielorganisation, in folgendem Format:

   ```
   systemId,to-org-id
   ```

   Angenommen, der ***`systemId`***-Parameter lautet **`1000010000`** und der ***`to-org-id`***-Parameter lautet **`3`**. In diesem Fall würde die CSV-Datei folgendermaßen aussehen:

   ```
   1000010000,3
   1000010020,1
   1000010010,4
   ```

Versionsgeschichte

Version 3-5.2.400	2013-10-31	Rüdiger Landmann

Rebuild with publican 4.0.0

Version 3-5.2	Wed Nov 28 2012	Hedda Peters

Deutsche Übersetzung fertiggestellt

Version 3-5.1	Sun Nov 4 2012	Terry Chuang

Übersetzungsdateien synchronisiert mit XML-Quelldateien 3-5

Version 3-5	Wed Sept 19 2012	Dan Macpherson

Finale Zusammenstellung für 5.5

Version 3-4	Fri Aug 31 2012	Athene Chan

BZ#839798 Kleine Änderung

Version 3-3	Fri Aug 24 2012	Athene Chan

BZ#839798 4.3 Beispiel wurde auf standardmäßiges Format geändert

Version 3-3	Fri Aug 24 2012	Athene Chan

BZ#839798 4.3 Beispiel wurde auf standardmäßiges Format geändert

Version 3-2	Fri Aug 24 2012	Athene Chan

BZ#826501 Änderungen nach QA-Prüfung implementiert.
BZ#884313 Änderungen nach QA-Prüfung implementiert.

Version 3-1	Fri Aug 17 2012	Athene Chan

BZ#848313 OpenSCAP-Kapitel "Anzeigen von SCAP-Ergebnissen" hinzugefügt

Version 3-0	Thu Aug 9 2012	Athene Chan

Staging zwecks Revision

Version 2-5	Wed Aug 1 2012	Athene Chan

BZ#839798 Kapitel über spacewalk-clone-by-date hinzugefügt
BZ#826501 Neue OpenSCAP-Informationen hinzugefügt

Version 2-0	Fri Jul 6 2012	Athene Chan

Vorbereitet für RHN Satellite 5.5 Release
BZ#826501 OpenSCAP-Kapitel hinzugefügt
OpenSCAP-Screenshots hinzugefügt

Version 1-5	Mon Aug 15 2011	Lana Brindley

Änderungen der z-Stream Release in y-Stream-Release eingebracht

Version 1-4	Mon Jun 20 2011	Lana Brindley

BZ#701900 - PAM-Authentifizierung

Version 1-3	Mon Jun 20 2011	Lana Brindley

BZ#714029 - Farbe in Abbildung korrigiert

Version 1-2	Wed Jun 15 2011	Lana Brindley

Vorbereitet für Übersetzung

Version 1-1	Fri May 27 2011	Lana Brindley

Änderungen von Übersetzern

Version 1-0	Fri May 6, 2011	Lana Brindley

Vorbereitet für Übersetzung

Version 0-15	Thu May 5, 2011	Lana Brindley

BZ#701818 - QE-Prüfung

Version 0-14	Mon May 2, 2011	Lana Brindley

BZ#248465 - QE-Prüfung

Version 0-13	Fri Apr 29, 2011	Lana Brindley

BZ#692295 - QE-Prüfung

Version 0-12	Mon Apr 18, 2011	Lana Brindley

BZ#691985 - Abbildung aktualisiert

Version 0-11	Mon Apr 18, 2011	Lana Brindley

BZ#691990 - QE-Prüfung

Version 0-10	Mon Apr 18, 2011	Lana Brindley

BZ#691985 - QE-Prüfung

Version 0-9	Thu Apr 14, 2011	Lana Brindley

Feedback nach technischer Überprüfung

Version 0-8	Wed Apr 13, 2011	Lana Brindley

BZ#692314 - QE-Prüfung
BZ#692294 - QE-Prüfung
BZ#692291 - QE-Prüfung
BZ#692290 - QE-Prüfung
BZ#691988 - QE-Prüfung
BZ#691986 - QE-Prüfung
BZ#691981 - QE-Prüfung

Version 0-7	Wed Mar 23, 2011	Lana Brindley

Vorbereitung für technische Überprüfung

Version 0-6	Mon Feb 19, 2011	Lana Brindley

RPMs
Boot-Geräte
Organisationen

Version 0-5	Fri Feb 18, 2011	Lana Brindley

Monitoring
PAM-Authentifizierung

Version 0-4	Mon Jan 10, 2011	Lana Brindley

Datensicherung und Wiederherstellung

Version 0-3	Fri Jan 7, 2011	Lana Brindley

Benutzerverwaltung
Vorwort
Automatische Synchronisation

Version 0-2	Wed Jan 5, 2011	Lana Brindley

Benutzerverwaltung

Version 0-1	Tue Jan 4, 2011	Lana Brindley

Neue Kapitelstruktur abgeschlossen

Version 0-0	Tue Dec 21, 2010	Lana Brindley

Erstellung eines neuen Dokuments aus dem ursprünglichen RHN Satellite Deployment-Handbuch

Stichwortverzeichnis

A

API

- Prüfscan, Durchführen von Prüfscans

B

Benutzer, Benutzerverwaltung

- deaktivieren, Hinzufügen, Deaktivieren und Löschen von Benutzerkonten
- E-Mail-Adresse ändern, Benutzerverwaltung
- hinzufügen, Hinzufügen, Deaktivieren und Löschen von Benutzerkonten
- löschen (nur RHN Satellite Server), Hinzufügen, Deaktivieren und Löschen von Benutzerkonten
- Passwort ändern, Benutzerverwaltung
- Rollen, Benutzerverwaltung

Benutzerrollen, Benutzerverwaltung

D

deaktivieren

- Benutzer, Hinzufügen, Deaktivieren und Löschen von Benutzerkonten

E

E-Mail-Adresse

- ändern, Benutzerverwaltung

F

Funktionsumfang, OpenSCAP-Funktionsumfang

H

hinzufügen
- Benutzer, Hinzufügen, Deaktivieren und Löschen von Benutzerkonten

K

Klonen einer Maschine
- spacewalk-clone-by-date, Klonen einer Maschine

L

löschen
- Benutzer (nur RHN Satellite Server), Hinzufügen, Deaktivieren und Löschen von Benutzerkonten

O

OpenSCAP, OpenSCAP, OpenSCAP-Funktionsumfang, Voraussetzungen, Durchführen von Prüfscans

P

PAM-Authentifizierung
- Implementierung, PAM-Authentifizierung

Passwort
- ändern, Benutzerverwaltung

Prüfscans, Durchführen von Prüfscans
- OpenSCAP, Durchführen von Prüfscans

Prüfung
- OpenSCAP, OpenSCAP

S

Satellite Administrator, Benutzerverwaltung

spacewalk-clone-by-date, Klonen einer Maschine

V

Voraussetzungen
- OpenSCAP, Voraussetzungen

W

Weboberfläche
- Prüfscans, Durchführen von Prüfscans

Website
- Benutzer, Benutzerverwaltung